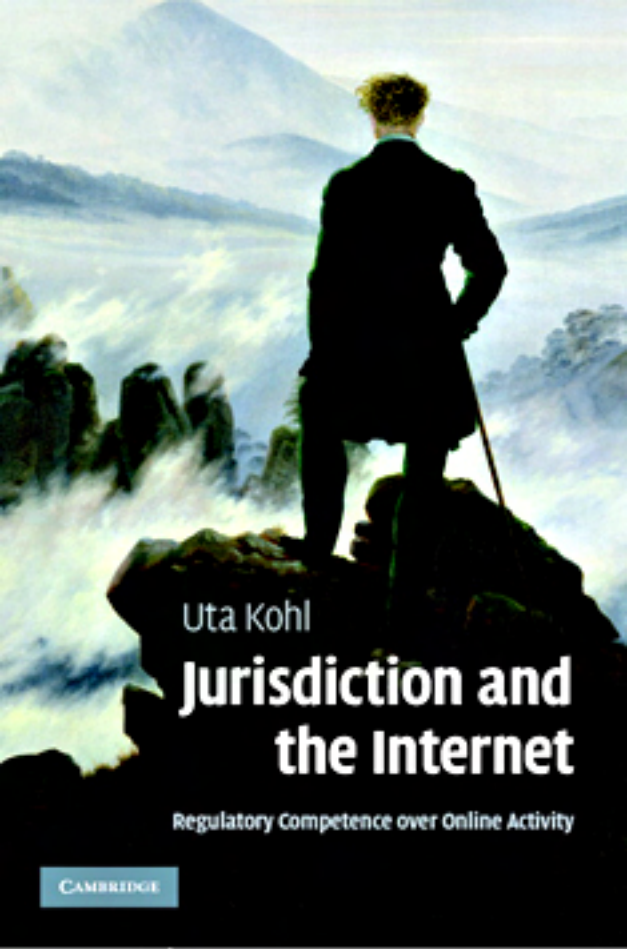

CAMBRIDGE www.cambridge.org/9780521843805

This page intentionally left blank

JURISDICTION AND THE INTERNET

This book examines how regulatory competence is allocated over online activity: which State has the right to regulate which site or online event? Who can apply their defamation or contract law, their obscenity standards, gambling or banking regulation, pharmaceutical licensing requirements or hate speech prohibitions to a site – and enforce these laws? Traditionally transnational activity has been 'shared out' between States with the aid of location-centric rules and these can be adjusted to suit the Internet. But can these rules be stretched indefinitely and what are the costs of squeezing global online activity into nation-state law? This book offers some uncomfortable insights into one of the most important debates on Internet governance, and will be of interest to students, academics, policy makers, legal practitioners and businesses who work in the field of e-commerce or Internet regulation.

UTA KOHL is a lecturer in law at the University of Wales, Aberystwyth.

JURISDICTION AND THE INTERNET

Regulatory Competence over Online Activity

UTA KOHL
University of Wales, Aberystwyth

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK
Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521843805

First published in print format 2007

ISBN-13 978-0-511-36620-8 eBook (EBL)
ISBN-10 0-511-36620-5 eBook (EBL)

ISBN-13 978-0-521-84380-5 hardback
ISBN-10 0-521-84380-4 hardback

CONTENTS

Preface and acknowledgments *page* ix
Table of cases xi
Table of statutes, regulations, directives and treaties xviii

1 Jurisdiction and the Internet 1

1. The global net versus national laws 1
   A. A story about eggs 1
   B. Mapping the legal landscape 3
   C. Who cares? 6
   D. A conservative approach 11
2. The building blocks 13
   A. Jurisdiction 13
   B. Public law versus private law 19
   C. The quest for the perfect link 20
3. Actual and possible solutions foreshadowed 24
   A. Territoriality: country-of-origin and country-of-destination 24
   B. The Achilles' Heel: limited enforcement jurisdiction 26
   C. More global law or a less global internet: a simple choice 28
   D. Code: a separate option? 30

2 Law: too lethargic for the online era? 33

1. National trademarks versus international domain names 33
2. The Internet's impact on law and regulation 35
   A. The qualitatively new legal problems 35
   B. The quantitatively new legal problems 37
   C. The severity of the problems 39
3. Legal reasoning and legal change 41
   A. Legal reasoning 41
   B. Judicial reasoning: continuity and change 43
   C. Legislative justification: change and continuity 45
4. The jurisdictional challenge 47
   A. Is a website enough? Two schools of thought 47

B. Conservatism: a mere result of the judiciary's limitations? 52
C. The best solution versus the least disruptive solution 56
5. Law as an engine of, or brake on, change 58
A. The floodgates argument 59
B. The futility argument 62
C. The cautious way forward 64

3 The tipping point in law 66

1. Contract law: unaffected by online transnationality? 66
2. The tipping point 69
A. Evolution of law versus the tipping point 69
B. Substantive justice versus formal justice 71
3. The evolution of jurisdictional rules in private cases 74
A. Adjudicative jurisdiction in consumer contracts: no gain without pain 74
B. Pre-Internet refinements 79
C. Internet refinements 82
4. The evolution of jurisdictional rules in public cases 87
A. Criminal jurisdiction 87
B. Pre-Internet refinements 89
The objective territoriality principle 89
The 'reasonable' effects doctrine 91
Return to a 'crude' effects doctrine 94
C. Internet developments 96
D. The common denominators 102
The possibility of concurrent jurisdiction 102
Insistence on enforcement jurisdiction 104
Lack of international consensus: moral and cultural values 107
5. The better path? 108

4 Many destinations but no map 111

1. Notice of foreign legal obligations 111
2. Foreseeability of foreign defamation law 115
A. Foreseeability and the rule of law 115
B. Absence of noticeable borders in cyberspace 117
C. Actual access, even if minuscule 119
D. Foreseeability of foreign law in respect of freely accessible sites 125
Foreseeability of all destinations 127
Foreseeability of foreign harm 129
Foreseeability of specifically targeted destinations 134
E. Two destination principles: their flaws and merits 138

3. Foreseeability of foreign criminal law 141
A. Common rules but multiple interpretations 141
B. Foreseeability and the territoriality principle 143
C. Foreseeability of all destinations 145
D. 'Reasonable foreseeability': some conclusions 149
4. Actually foreseeing and knowing foreign law 153
A. Actual notice and the effectiveness of law 153
B. Traditional methods of publication of law 157
C. The failure of traditional methods in the online world 159
5. An afterthought 163

5 The solution: only the country of origin? 164

1. The *exclusive* country-of-origin approach 164
2. Online gambling: foreign providers' local activities 167
A. The general rejection of the exclusive country-of-origin approach 167
Netherlands and Germany 167
European Union 168
United States 169
WTO and GATS 171
Australia 173
New Zealand 174
B. The exclusive country-of-origin approach and its flaws 175
The UK Gambling Act 2005 175
Loss of economic rewards 176
Forum-shopping and the race to the bottom 178
Shift of regulatory burden 181
No protection from harmful foreign content 182
Lowest common denominator 184
The special case of the Electronic Commerce Directive 184
3. Online gambling: local providers' foreign activities 190
A. Lack of cooperation in non-harmonised public law 190
B. The UK and Australia: good neighbours 193
4. An example to follow? 197

6 The lack of enforcement power: a curse or a blessing? 199

1. Limited enforcement power: a blessing in disguise 199
2. Enforceability and legal compliance 203
A. Enforceability, not enforcement, matters 203
B. 'Voluntary' compliance without the threat of enforcement 206
C. Enforceability and why it really matters 207
3. Upholding local law despite foreign violations 210

A. Cooperation in private law 210
Cooperation and regulatory restraint 212
Two interpretations of the 'public policy' exception 214
B. No cooperation in public law 218
The 'public law' taboo 218
Lack of power or lack of will? 221
C. Unilateral enforcement strategies 225
Symbolic prosecution without enforcement 225
Imposition of penalty on related local persons 226
Analogous prohibitions imposed on local intermediaries and end-users 227
Prohibition of supportive services by local actors 228
Blocking of foreign illegal content 229
4. The public–private law dichotomy and its lessons for cooperation 230
A. 'Public' and 'private' international law 231
B. The public–private law spectrum 233
C. Underlying concern: foreign State interest and involvement 238
Public versus private complainants 240
Public versus private cause of action 242
Public versus private remedy 245
The paradox 248
5. The future of cooperation 251

7 A 'simple' choice: more global law or a less global Internet 253

1. The hidden choice 253
2. More global law 258
A. Harmonisation of competence rules? 259
B. Substantive harmonisation by design 262
Harmonisation through treaty 263
Harmonisation through deregulation 265
C. Substantive harmonisation by default 270
The country-of-destination approach 271
The country-of-origin approach 275
3. A less transnational Internet 278
A. Zoning in the country of origin 278
B. Zoning in the country of destination 283
4. Making the choice: a value judgment 287

Bibliography 291
Index 312

PREFACE AND ACKNOWLEDGMENTS

> If a thing is worth doing, it is worth doing badly.
>
> G. K. Chesterton, *What's Wrong with the World*

When I first came across Johnson and Post's article, 'Law and Borders – The Rise of Law in Cyberspace' (1996), in 1998, it impressed me. The authors seem to prove quite conclusively that States could not possibly, in all rationality, apply their laws to online activity and that this new cyberspace was completely beyond their legitimate and actual supervision. And yet, at the same time, the first cases were emerging where States did exactly that. Over the following years, while investigating competence questions in cyberspace, the article has stayed with me and my views on it have almost come full circle: from being fascinated by it and utterly convinced of its accuracy, to rejecting most of it, to finally admiring the brilliance that lies in the confident simplicity of its core ideas and in its provocative imperfections. If this book can follow suit, it does well.

Researching for, and writing, this book was a humbling experience. I was left, at every stage, with the feeling that there was so much more to read and know. Being a Jack-of-all-trades is perhaps partly a genetic predisposition and partly unavoidable given the nature of the competence inquiry, spanning across most substantive legal fields. However, in this case no doubt it was mainly down to the ambition to understand and explain the 'big picture' – the picture of how national law and the transnational Internet can be reconciled – based on the conviction that there is a need for such understanding. Yet still I am only too conscious of the specialists who will read this book and all the imperfections they may unearth.

This book may be read from cover to cover, but it need not be. Although each chapter builds upon the preceding ones, they also stand quite comfortably on their own. (Indeed Chapter 2 and Chapter 3 are revised versions of two earlier articles, 'Legal Reasoning and Legal

Change in the Age of the Internet – Why the Ground Rules Are Still Valid' (1999) 7 IJLIT 123 and 'Eggs, Jurisdiction and the Internet' (2002) 51 ICLQ 555, and Chapter 4 builds on some of my previous writing on online defamation; see the bibliography.) An abbreviated version of the main arguments made in this book is provided in Chapter 1, which also sets out basic background 'data': the key problem, its relevance and the general legal framework. All the other chapters present a general argument in a specific legal context in order to make the sheer volume of material manageable and to focus the discussion. Thus, Chapter 2 looks at the nature of legal change and reasoning in the general context of the conflict between transnational domain names and national trademarks. Chapter 3 examines the dangers of fine-tuning legal rules beyond a certain point in the context of the US 'targeting' approach and EU consumer contracts (in comparison with online crime). Chapter 4 examines the pros and cons of the outright and the moderate country-of-destination approaches by reference to online defamation (again compared with online crime). Chapter 5 discusses the exclusive country-of-origin approach illustrated by gambling regulation and the Electronic Commerce Directive. Chapter 6 analyses questions of enforcement and enforceability in the context of the *Yahoo* saga. And, finally, Chapter 7 examines the two fundamental regulatory options open to States, using spam regulation as the specific example.

There are many people who helped me in very different ways to write this book, but a few stick out: my parents, Birgit Wacks and Andreas Kohl, who taught me the importance of finishing what you start; my PhD supervisor, Eugene Clark, whose infectious energy made it difficult to sustain any pessimism or writing fatigue at the worst of times; my colleagues and friends, Christopher Harding and Naomi Salmon, who – invariably over coffee – shared my tribulations and provided intellectual stimulation, much fun and a sense of perspective on life generally; the editing team of Cambridge University Press, Finola O'Sullivan and Richard Woodham, who never made me feel late, even when I was very late; and last but not least Ryszard Piotrowicz, whose substantive feedback, proofreading and general encouragement made all the difference. Thank you.

TABLE OF CASES

800-Flowers Trade Mark [2000] FSR 697 *page* 50
ACLU v. Reno, 929 F Supp 824 (ED Pa 1996), affirmed in Reno v. ACLU, 521 US 844 (1997) 60, 64, 288
Adams v. Cape Industries plc [1990] Ch 433 (CA) 74, 209
AG (UK) v. Heinemann Publishers Australia Pty Ltd (1988) 165 CLR 30 220, 222, 235, 238, 239, 240, 241, 243, 244, 249
AG of New Zealand v. Ortiz [1984] AC 1, affirming AG of New Zealand v. Ortiz [1982] QB 349 222, 236, 237, 241
Albaforth, The (Cordoba Shipping Co. Ltd v. National State Bank, Elizabeth, New Jersey) [1984] 2 Lloyds Reports 91 112
Alcoa Case (US v. Aluminium Company of America), 148 F 2d 416 (1945) 91, 144
ALS Scan Inc. v. Digital Serv Consultants Inc., 293 F 3d 707 (4th Cir. 2002) 49, 136
Arzneimittelwerbung im Internet (BGH, 30 March 2006, I ZR 24/03) 166, 179, 186
Atcheson v. Everitt (1775) I Cowp 382 231
Ayers v. Evans (1981) 56 FLR 335 240, 241, 242, 246
Banco Nacional de Cuba v. Sabbatino, 376 US 398 (1964) 221
Bank voor Handel en Scheepvaart NV v. Slatford [1953] 1 QB 248 (CA) 222, 243
Barcelona Traction Case: Case Concerning the Barcelona Traction, Light and Power Company, Ltd (Belgium v. Spain), Preliminary Objections [1964] ICJ Reports 6 92, 226
Bata v. Bata (1948) WN 366 119
Bensusan Restaurant Corp. v. King, 937 F Supp 295 (SDNY 1996) 49, 53, 54
Berezovsky v. Michaels [2000] 1 WLR 1004 112, 120, 123
Bier v. Mines de Potasse d'Alsace, Case 21/76 [1976] ECR 1735 124
Blumenthal v. Drudge, 992 F Supp 44 (1998) 135
Bodil Lindqvist, Case C-101/01 [2004] 1 CMLR 20 125, 276
Bonnier Media Ltd v. Greg Lloyd Smith and Kestrel Trading Corp. (Court of Session, Scotland, 1 July 2002), www.scotcourts.gov.uk/opinionsv/dru2606.html 50, 137
Brandenburg v. Ohio, 395 US 444 (1969) 107, 207
British Aeropace plc v. Dee Howard Co. [1993] 1 Lloyds Reports 368 75

British Airways Board v. Laker Airways Ltd [1984] 1 QB 142 (CA) 246
British Nylon Spinners v. Imperial Chemical Industries [1953] Ch 19 (CA) 219
Brokaw v. Seatrain UK Ltd [1971] 2 QB 476 (CA) 241
Bullfrog Films Inc. v. Wick, 646 F Supp 492 (CD Cal. 1986) 216
Cable News Network LP v. CNNews.com, 56 Fed Appx 599 (4th Cir. 2003), affirming Cable News Network LP v. CNNews.com, 177 F Supp 2d 506 (ED Va 2001) 51, 86, 149
Calder v. Jones, 465 US 783 (1984) 133
Carnival Cruise Lines Inc. v. Shute, 499 US 585 (1991) 78
Citron v. Zündel (No. 4) (2002) 41 CHRR D/274 107, 153
Commission v. UK, Case C-222/94 [1996] ECR I-4025 181, 188
Compuserve v. Patterson, 89 F 3d 1257 (6th Cir. 1996) 54
Connor v. Connor [1974] 1 NZLR 632 241
Cotton v. King [1914] AC 176 (PC) 225
Criminal Proceedings against Piergiorgio Gambelli, Case C-243/01 [2003] ECR I-13031 168, 169, 172, 176, 177, 182, 187, 277
Cybersell Inc. v. Cybersell Inc., 130 F 3d 414 (9th Cir. 1997) 49
Desai v. Hersh, 719 F Supp 670 (ND Ill. 1989) 216
Deutscher Apothekerverband eV v. 0800 Doc Morris NV, Case C-322/01 [2003] ECR I-14887 166, 179, 186
Dietrich v. Queen (1992) 177 CLR 292 41
Digital Equipment Corp. v. Altavista Technology Inc., 960 F Supp 456 (D Mass. 1997) 48, 51, 53
Distillers Co. (Biochemicals) Ltd v. Thompson [1971] AC 458 (PC) 133
Dluhos v. Strasberg, WL 1683732 (DNJ 2005) 49
Dow Jones & Co. Inc. v. Gutnick [2002] HCA 56, affirming Gutnick v. Dow Jones & Co. Inc. [2001] VSC 305 13, 39, 112, 120, 121, 123, 125, 126, 127, 128, 129, 130, 133, 135, 136, 138, 139, 140, 152, 157, 160, 164, 178, 180, 212, 225, 254, 255, 288
Dow Jones & Co. Inc. v. Harrods Ltd and Mohamed Al Fayed, 237 F Supp 2d 394 (2002) 121
Ducharme v. Hunnewell, 411 Mass 711 (1992) 247
Duke of Brunswick and Luneberg v. Harmer (1849) 14 QB 184 120
Emanuel v. Symon [1908] 1 KB 302 (CA) 74
ESAB Group Inc. v. Centricut Inc., 126 F 3d 617 (4th Cir. 1997) 136
Euromarket Designs Inc. v. Crate & Barrel Ltd, 96 F Supp 2d 824 (ND Ill. 2000) 49, 84, 152
Euromarket Designs Inc. v. Peters [2000] ETMR 1025 50, 138
Firth v. State of New York, 775 NE 463 (Ct App 2002) 120
Foster v. Driscoll [1929] 1 KB 470 (CA) 248
Fothergill v. Monarch Airlines [1981] AC 251 (HL) 116
Gertz v. Robert Welch Inc., 418 US 323 (1974) 133

Government of India v. Taylor [1955] AC 491 (HL) 241, 245
Green v. Mason, 996 F Supp 394 (1998) 81
Groppera Radio AG v. Switzerland (1990) 12 EHRR 321 37
GTE New Media Services Inc. v. Bellsouth Corp., 199 F 3d 1343 (D Co 2000) 85
Halean Products Inc. v. Beso Biological, 43 USPQ (BNA) 1672 (1997) 83
Hanson v. Denckla, 357 US 235 (1958) 81
Harrods Ltd v. Dow Jones & Co. Inc. [2003] EWHC 1162 (QB) 112, 121, 130, 140, 152
Hartford Fire Insurance Co. v. California, 509 US 764 (1993) 94, 145
Haynsworth v. The Corporation, 121 F 3d 956 (5th Cir. 1997) 78
Hearst Corp. v. Goldberger, WL 97097 (SDNY 1997) 51, 55
Heroes Inc. v. Heroes Foundation, 958 F Supp 1 (DDC 1996) 49, 53
Hilton v. Guyot, 159 US 113 (1895) 80, 224
Hoath v. Connect Internet Services [2006] NSWSC 158 36
Holland Casino v. Paramount Holdings (District Court, Utrecht, 27 February 2003) 167
Huntington v. Attrill [1893] AC 150 (PC) 232, 238, 240, 241, 242, 243, 245, 246
Huntington v. Attrill, 146 US 657 (1892) 221, 222, 232, 245
Huth v. Huth [1915] 3 KB 32 133
Inset Systems Inc. v. Instruction Set Inc., 937 F Supp 161 (D Conn. 1996) 49, 51, 54, 83
International Shoe Co. v. Washington, 326 US 310 (1945) 79, 80, 81, 90
Island of Palmas (The Netherlands v. United States of America) (1928) 2 RIAA 829 27, 200
ITP Solar Technologies Inc. v. TAB Consulting Inc., 413 F Supp 2d 12 (DNH 2006) 49
Jabbour v. Custodian of Israeli Absentee Property [1954] 1 WLR 139 80
Jaensch v. Coffey (1984) 155 CLR 549 41
Jenner v. Sun Oil Co. (1952) 2 DLR 526 122
Jeremy Jones and Members of the Committee of Management of the Executive Council of Australian Jewry v. Frederick Töben (Australian Human Rights and Equal Opportunities Commission, 5 October 2000), affirmed in Jones v. Töben [2002] FCA 1150 101, 107
Kamer van Koophandel en Fabrieken voor Amsterdam v. Inspire Art Ltd, Case C-167/01 [2003] ECR I-10115 180
Keeton v. Hustler Magazine Inc., 465 US 770 (1984) 124
Kitkufe v. Olaya Ltd, ACWSJ LEXIS 84447 (Ontario Court of Justice, 1998) 122
Kleinwort Benson v. Glasgow [1999] 1 AC 153 (HL) 74
Konsumentombudsmannen (KO) v. De Agostini (Svenska) AB and TV-Shop i Sverige AB (C-35/95 and C-36/95), Case C-34/95 [1997] ECR I-3843 186
Kroch v. Rossell [1937] 1 All ER 725 121, 130, 133
Kunstsammlung zu Weimar v. Elicofon, 678 F 2d 1150 (2d Cir. 1982), affirmed 536 F Supp 829 (EDNY 1981) 241, 243

Kuwait Airways Corp. v. Iraqi Airways Co. [2002] UKHL 19 209, 215
Laker Airways Ltd v. Pan American Airways Inc., 604 F Supp 280 (DDC 1984) 216
Lee Teck Chee v. Merrill Lynch International Bank Ltd [1998] Current Law Journal 188 122
Lee v. Wilson and Mackinnon (1934) 51 CLR 276 119
Lewis v. King [2004] EWCA Civ 1329 (CA), affirming King v. Lewis [2004] EWHC 168 112, 121, 122, 128, 130, 140
LICRA and UEJF v. Yahoo! Inc. and Yahoo France (Tribunal de Grande Instance de Paris, 20 November 2000), affirming LICRA and UEJF v. Yahoo! Inc. and Yahoo France (Tribunal de Grande Instance de Paris, 22 May 2000) 99, 100, 105, 140, 145, 160, 201, 202, 213, 226, 227, 245, 283
LICRA and UEJF v. Yahoo! Inc. and Yahoo France (Tribunal de Grande Instance de Paris, 11 August 2000), www.foruminternet.org/actualites/lire.phtml?id=273, translations www.lapres.net/yahweb.html 202
LICRA v. Yahoo! Inc., 126 SCt 2332 (Mem) (2006) 203
Lipohar v. R (1999) 168 ALR 8 14, 105, 141, 223, 224
Liu v. Republic of China, 892 F 2d 1419 (9th Cir. 1989) 221
Lorentzen v. Lydden & Co. Ltd [1942] 2 KB 202 237
Lotus Case: The Case of the SS 'Lotus' (France v. Turkey) (1927) PCIJ Reports, Series A, No. 10 16, 25, 26, 89–91, 142, 200
Loucks v. Standard Oil Co. of New York, 120 NE 198 (NY 1918) 215
Loutchansky v. Times Newspapers Ltd [2001] EWCA Civ 1805 120, 123
Macquarie Bank v. Berg [1999] NSWSC 526 85, 108, 152
MacShannon v. Rockware Glass Ltd [1978] 1 All ER 625 122
Mannington Mills v. Congoleum Corp., 595 F 2d 1287 (1979) 145
MARITIM Trade Mark, Re [2003] ILPr 17 50
Maritz Inc. v. Cybergold Inc., 947 F Supp 1328 (ED Mo 1996) 40, 54, 83
McDonough v. Fallon McElligott Inc., 40 USPQ 2d (BNA) 1826 (SD Cal. 1996) 50
McGee v. International Life Insurance Co., 355 US 220 (1957) 80
Mecklermedia Corp. v. DC Congress GmbH [1998] 1 All ER 148 48
Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd, 545 US 125 (2005) 227
Millennium Enterprises Inc. v. Millennium Music LP, 33 F Supp 2d 907 (D Or. 1999) 49, 84, 85
Moore v. Mitchell, 30 F 2d 600 (1929) 220
Moshe D, Re (Italian Court of Cassation, 17 December 2000), www.cdt.org/speech/international/20001227italiandecision.pdf 122
Municipal Council of Sydney v. Bull [1909] 1 KB7 243
National Sporttotaliser Foundation v. Ladbrokes Ltd (District Court, The Hague, 27 January 2003), www.rechspraak.nl 167
New York Times Co. v. Sullivan, 376 US 254 (1964) 133
Nottebohm Case (Liechtenstein v. Guatemala) [1955] ICJ Reports 4 93
Ocean Sun Line Special Shipping Co. Inc. v. Fay (1988) 165 CLR 197 (HL) 82

Panavision Intern LP v. Toeppen, 141 F 3d 1316 (1998) 49
Pennoyer v. Neff, 95 US 714 (1887) 79
People v. World Interactive Gaming Corp., 714 NYS 2d 844 (1999) 96, 97, 102, 103, 104, 107, 148, 149, 152, 170, 228
People of Vacco v. Lipsitz, 663 NYS 2d 468 (NY Sup. 1997) 48
Perrin v. UK (ECHR, 18 October 2005, Application No. 5446/03)
Peter Buchanan Ltd and Macharg v. McVey [1955] AC 516 (Ir HC) 241, 242
Phrantzes v. Argenti [1960] 2 QB 19 (CA) 215
Pinding v. National Broadcasting Corp. (1985) 14 DLR (4th) 391 122
Playboy Enterprises Inc. v. Chuckleberry Publishing Inc., 939 F Supp 1032 (SDNY 1996) 48, 54, 55, 60, 62, 151
Powell v. Gelston [1916] 2 KB 615 133
Prince plc v. Prince Sports Group Inc. [1998] FSR 21 34
Pullman v. Walter Hill & Co. Ltd [1891] 1 QB 524 133
R v. Burdett (1820) 4 B & Ald 115 151
R v. Catanzariti (1995) 65 SASR 201 95
R v. Felix Somm, CEO of CompuServe GmbH (AG München I, 17 November 1999 – 20 Ns 465 Js 173158/95), www.computerundrecht.de/1672.html 103
R v. Harden [1963] 1 QB 8 143, 219
R v. Lipohar (1999) 168 ALR 8 95, 96
R v. Manning [1999] 2 WLR 430 105
R v. Perrin [2002] EWCA Crim 747 98, 99, 140, 145, 151, 164, 280
R v. Timothy K and Yahoo! Inc. (Tribunal de Grande Instance de Paris, 26 February 2002, No. 0104305259), www.foruminternet.org/actualites/lire.phtml?id=273/ 100, 102, 145, 160, 161, 244
R v. Treacy [1971] AC 537 151, 165
Rainbow Warrior (New Zealand v. France) 74 ILR 241 191
Raulin v. Fisher [1911] 2 KB 93 240, 244
Rayner v. Davies [2002] EWCA Civ 1880 75
Regazzoni v. KC Sethia (1944) Ltd [1958] AC 301 (HL) 235, 248, 249
Regie National des Usines Renault SA v. Zhang (2002) 76 ALJR 551 (HC) 15, 113
Reno v. ACLU, 521 US 844 (1997), affirming ACLU v. Reno, 929 F Supp 824 (ED Pa 1996)
SA Consortium General Textiles v. Sun and Sand Agencies Ltd [1978] QB 279 (CA) 246
Sanitec Industries Inc. v. Sanitec Worldwide Ltd, 376 F Supp 2d 571 (D Del. 2005) 49
Schöner Wetten (BGH, 1 April 2004, I ZR 317/01) (2004) *Computer und Recht* 613 168
Schimmelpenninck, Re, 183 F 3d 347 (5th Cir. 1999) 215
Shaffer v. Heitner, 433 US 186 (1977) 80
Shamsuddin v. Vitamin Research Products, 346 F Supp 2d 804 (D Md 2004) 84, 85

Shetland Times Ltd v. Wills [1997] FSR 604 36
Shevill v. Presse Alliance SA, Case C-68/93 [1995] ECR I-415 25, 124, 125, 131
Socialist Labor Party v. Gilligan, 406 US 583 (1972) 205
Sosa v. Alvarez-Machain, 542 US 692 (2004) 200
Spiliada Maritime Corp. v. Cansulex Ltd (The Spiliada) [1987] AC 40 (HL) 82
Staples v. US, 511 US 600 (1994) 158, 162, 170
State v. Truesdale, 152 F 3d 443 (5th Cir. 1988)
State of Minnesota v. Granite Gate Resorts Inc., 568 NW 2d 715 (1997), affirming State of Minnesota v. Granite Gate Resorts Inc., WL 767431 (Minn. 2d Dist. 1996) 148, 161
State of Missouri v. Coeur D'Alene Tribe, 164 F 3d 1102 (1999) 170
State of Missouri v. Interactive Gaming & Communications Corp., WL 33545763 (Mo Cir. 1997) 170
State of Norway's Application, Re [1990] 1 AC 723 (HL) 223
Stomp Inc. v. Neato LLC, 61 F Supp 2d 1074 (CD Cal. 1999) 84
Sunday Times v. UK (No.1) (1979) 2 EHRR 245 145
Tech Head Inc. v. Desktop Service Center Inc., 105 F Supp 2d 1142 (D Or. 2000) 152
Ticketmaster Corp. v. Tickets.com Inc., WL 525390 (CD Cal. 2000) 36, 152
Timberlane Lumber Co. v. Bank of America, 549 F 2d 597 (1976) 93, 145
Töben (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624 100, 101, 105, 106, 140, 145, 160, 225
Toys 'R' Us Inc. v. Step Two, 318 F 3d 446 (3rd Cir. 2003) 29, 34, 49
Trail Smelter Arbitration (United States of America v. Canada) (1938) 3 RIAA 1905 191
Turner Entertainment Co. v. Degeto Film GmbH, 25 F 3d 1512 (11th Cir. 1994) 215
Twentieth Century Fox Film Corp. v. iCraveTV, US Dist. LEXIS 1013 (WD Pa, 28 January 2000) 153
Underhill v. Hernandez, 168 US 250 (1897) 221
United Cutlery Corp. v. NFZ Inc., WL 22851946 (D Md 2003) 84
United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services (WTO Appellate Body, 7 April 2005, WT/DS285/AB/R), on appeal from WTO Panel (10 November 2004, WT/DS285/R) 171, 172
Unzulässiges Online-Glücksspielangebot (OLG Hamburg, 19 August 2004, 5 U 32/04) (2004) 12 *Computer und Recht* 925 167, 168, 169
US v. American Sports Ltd, 286 F 3d 641 (3rd Cir. 2002) 102, 104, 105, 170, 171, 206
US v. Cohen, 260 F 3d 68 (2d Cir. 2001) 170, 172
US v. General Electric Co., 82 F Supp 753 (1949) 92
US v. Harden (1963) 41 DLR 2d 721 241
US v. Inkley [1989] QB 255 (CA) 219, 243, 249

US v. Ivey (1996) 139 DLR (4th) 570 246
US v. Ross, WL 782749 (SDNY 1999) 169
Vita Food Products Inc. v. Unus Shipping Co. [1939] AC 277 (PC) 67
Voth v. Manildra Flour Mills (1990) 171 CLR 538 133, 137
Weir v. Lohr (1967) 65 DLR (2d) 717 243, 246
Williams & Humbert v. W & H Trade Marks [1986] AC 368 (HL) 219, 241, 249
Worldwide Volkswagen Corp. v. Woodson, 444 US 286 (1980) 36, 82
Yahoo! Inc. v. LICRA and UEJF, 433 F 3d 1199 (9th Cir. 2006), affirming Yahoo! Inc. v. LICRA and UEJF, 379 F 3d 1120 (9th Cir. 2004), reversing Yahoo! Inc. v. LICRA and UEJF, 169 F Supp 2d 1181 (ND Cal. 2001), reversing Yahoo! Inc. v. LICRA and UEJF, 145 F Supp 2d 1168 (ND Cal. 2001) 99, 103, 104, 199–252, 273, 280
Young v. New Haven Advocate, 315 F 3d 256 (4th Cir. 2002), reversing Young v. New Haven Advocate, 187 F Supp 2d 498 (WD Vir. 2001) 49, 135, 136, 138, 140
Zündel v. Canada (1999) 175 DLR (4th) 512 107
Zippo Manufacturing Co. v. Zippo Dot Com Inc., 952 F Supp 1119 (WD Pa 1997) 48, 49, 50, 83, 84, 85, 86, 87, 118, 119, 137, 140

TABLE OF STATUTES, REGULATIONS, DIRECTIVES AND TREATIES

Australia

Crimes Act 1900 (NSW)
  s.10C *page* 95
  s.578C 98
Foreign Antitrust Judgments (Restriction of Enforcement) Act 1979 (Cth) 246
Interactive Gambling Act 2001 (Cth) 173
  Division 3
  s.3 173, 174
  s.8 173
  s.9A 194
  s.9B 194
  s.14 173
  s.15 173
  s.15A 173, 194, 196
Racial Discrimination Act 1975 (Cth) 101
  s.18C 108
Spam Act 2003 (Cth) 271
  s.7 272
  s.16 272

Canada

Human Rights Act 1985
  s.13(1) 106, 108

France

New Code of Civil Procedure (Nouveau Code de Procédure Civile) 99
  Arts. 808 and 809 202
Penal Code (Code Pénal) 244
  R-645-1 227
  R-645-2 108

Germany

Criminal Code
s.130 108
s.131 108

Italy

Law No. 401 of 13 December 1989
Art. 4 168, 227

New Zealand

Gambling Act 2003 174, 286
s.4 174
s.9(2) 174
s.15 174
s.16(1) 174, 228
s.19(1) 174

United Kingdom

Civil Procedure Rules 1998
r.6.15 75
Crime (International Co-operation) Act 2003 192
Electronic Commerce (EC Directive) Regulations 2002
reg.3(1) 168
Gambling Act 2005 166, 193, 197
s.1(c) 183
s.4 175
s.5(2) 184
s.5(3) 184
s.33 182, 189
s.33(1) 175
s.33(2) 175
s.36 175, 183, 189
s.36(3) 175
s.36(4) 175
s.36(5) 175
s.44 191, 194, 196
s.44(2) 194

s.46 183
s.48 183
Obscene Publications Act 1959
s.2(1) 98
Privacy and Electronic Communications (EC Directive) Regulations 2003 58
reg.22
Protection from Harassment Act 1997
s.3 244
Unfair Terms in Consumer Contracts Regulations 1999
reg.9 67

United States

Communications Decency Act 1996 64
§230 228
Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003
266, 272, 277
§5(a) 272
Digital Millennium Copyright Act 1998
Title 1 64
New York Penal Code
§225-05 228
Interstate Horse Racing Act 1978 172
Sherman Antitrust Act 1890 91
15 United States Code
§7704 272
18 United States Code
§1030(e) 272

EC Directives and Regulations

Copyright Directive 2001/29/EC
Art. 6 64
Credit Institutions Directive 89/646/EEC 186
Data Protection Directive 95/46/EC 125, 275, 276
Art. 4 175, 189, 227, 276
Art. 25 227
Direct Insurance other than Life Assurance Directive 92/49/EEC 186
Distance Selling Directive 97/7/EC 69
Electronic Commerce Directive 2000/31/EC 69, 197, 276
Recital 16 168
Art. 1(5) 168

Art. 2(c) 180
Art. 2(h) 185
Art. 3(1) 187, 190
Art. 3(2) 185, 189
Art. 3(4) 186, 188
Arts. 12–15 228
Art. 18 188
Art. 19 188
Investment Services in Securities Directive 93/22/EEC 186
Privacy and Electronic Communications Directive 2002/58/EC 57, 58, 69, 275, 276, 277
Recital 42 258
Art. 13(1) 275
Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001
Recital 11 72
Art. 2(1) 74
Art. 5(3) 124, 131
Art. 15(1) 76, 77, 114, 118, 119, 137, 140
Art. 16 76
Art. 23 67, 75
Television without Frontiers Directive 89/522/EC (revised by 97/36/EC) 186
Art. 2a(1) 186, 189
Art. 2(1) 181, 187, 188

Treaties, Protocols, Model Laws and Declarations

Agreement between the Government of Australia and the Government of the United Kingdom of Great Britain and Northern Ireland providing for the Reciprocal Recognition and Enforcement of Judgments in Civil and Commercial Matters (1990) 211
Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (1968)
Art. 5(3) 25
Art. 13(3) 75
Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) 192
Convention between the Member States of the European Communities on the Enforcement of Foreign Criminal Sentences (1991) 250
Convention on Mutual Assistance in Criminal Matters between Member States of the European Union (2000) 193
Council of Europe Cybercrime Convention (2001) 263, 264

Preamble 264
Chapter III 192
Art. 9 227
Arts. 23–35 201
Additional Protocol to the Cybercrime Convention, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2002) 217, 263, 264
Declaration on Freedom of Communication on the Internet (2003) 255, 256, 268
Principle 1 255
Principle 2 268
Principle 3 256, 286
Declaration on Freedom of Political Debate in the Media (2004) 255
EC Treaty/Treaty of Rome (1957)
Art. 28 185
Art. 43 168
Art. 45 169
Art. 49 168, 185
Art. 226 188
Art. 227 188
General Agreement on Trade in Services (GATS)
Art. 16 172
Art. 14(a) 172
Hague Conference on Private International Law Convention on Choice of Court Agreements (2005) 67
International Convention for the Suppression of the Financing of Terrorism (1999)
Art. 10 191
Montevideo Convention on Rights and Duties of States (1933)
Art. 1 8
Art. 8 191
Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000)
Art. 10 201
Rome Convention on the Law Applicable to Contractual Obligations (1980)
Art. 3 67
Art. 4 67
Art. 5 75
Art. 7 67, 105
Treaty of Amsterdam on the European Union (1997) 250
UN Convention on the Use of Electronic Communications in International Contracts (2005) 263
UNCITRAL Model Law on Electronic Signatures (2001) 263
UNCITRAL Model Law on Electronic Commerce (1996) 263

1

Jurisdiction and the Internet

1. The global net versus national laws

A. A story about eggs

A long time ago hens did not lay white or brown eggs but eggs in primary colours: red, yellow and blue.[1] Since, depending on the colour of the eggs, their taste and quality varied, the farming industry split into red, yellow and blue industries catering for different markets. Those industries which dealt with the respective eggs became over the years highly competitive. And what was initially no more than a common understanding, namely, that hens laying red eggs belonged to the red industry, while hens laying blue and yellow eggs belonged to the blue and yellow industries, turned over the years into customary egg law, with each industry having its clearly demarcated area of competence. As it happened, due to interbreeding, some hens normally laying, for example, red eggs would very occasionally lay purple or orange eggs. These eggs presented a problem, albeit not a severe one, as they remained very much the exception. Hens laying blue eggs were kept apart from hens laying red eggs and from those laying yellow eggs. Nevertheless, solutions to these problematic eggs had to be found. On occasions the red, blue or yellow industries would unilaterally declare, but only after close analysis and in accordance with their own complex rules about subtle colour variations (known as conflicts-of-egg law) that the egg in question belonged to its industry or to one of the other industries. These decisions were generally but not always accepted by the other industries. In respect of particularly big eggs there was a consensus at the higher farming level about the rules on who had a right to them. Again, these rules were equally complex and occasionally gave rise to

[1] This story was inspired by Tony Bradney, 'Law Schools and the Egg Marketing Board' (2001) 22 *SPTL Reporter* 1, and first published in 'Eggs, Jurisdiction and the Internet' (2002) 51 *International and Comparative Law Quarterly* 555.

arguments, but all in all the hen industry lived in peace and harmony for a long time.

And then something happened, what can only be called a miracle of nature. Hens could be fertilised through the air. While this was in itself not a problem and indeed made breeding hens so much easier and produced stronger, healthier hens with better, bigger and tastier eggs, the hen industry was in deep shock. Sure enough, the number of discoloured eggs increased drastically and, with it, the burden on the industries to work out which egg belonged to whom. But not only that, the frequent interbreeding produced totally new colour variations, meaning that the traditional rules had to be further and further refined, leading to what must have seemed totally arbitrary results. The teams of colour experts increased. Universities taught whole degrees on eggs and colours. Research on how to optimise and improve the solutions to allocating the non-primary coloured eggs was booming. Meetings between the red, blue and yellow industries took place frequently and yes, they did agree on further common rules, even in relation to the small eggs, for working out which one belonged to whom. Of course, every industry was very concerned about its own interest, none wanting to surrender too many eggs to the others. In an attempt to mitigate the uncontrolled and uncontrollable interbreeding, they built high walls around their hen farms, but to no avail. They also resorted to keeping eggs which they knew belonged to one of the other industries, which then caused more arguments and even reprisals. But one fact stubbornly remained: there was a constant relentless increase in non-primary coloured eggs, and their relative proportion to primary coloured eggs rose and rose. And these eggs were hardly distinguishable from one another in terms of quality or taste.

It took the farming industry a long time to acknowledge that its system of dividing the non-primary coloured eggs had broken down. Some even questioned whether it still made sense to divide eggs according to colour at all. But they were laughed at. The industries, though, finally grudgingly admitted to themselves that they were wasting time and effort to try to distinguish between eggs that could not really be distinguished. They had to find a new and more efficient way of distributing control over these difficult eggs. Some suggested a new industry dedicated entirely to these eggs. Yet, what happened between then and the time when all eggs became brown or white remains a mystery.

History repeats itself. Today it is no longer the issue which non-primary coloured egg belongs to which hen industry; the issue is

which transnational event or activity belongs to, or should be regulated by, which State. Is it France or Japan or Australia which has the right to regulate a transnational event which is not quite French, Japanese or Australian but a bit of each? And today it is not a miracle of nature which has thrown the traditional rules into disarray and questions their viability, but a miracle of science, the Internet. The number of transnational events is not only skyrocketing but gives rise to colour variations not known before. Finally, States are today struggling with accommodating these difficult events within their allocation rules based on location, so much so that there have been some calls to abandon the territorially-based system of regulation.

B. Mapping the legal landscape

This book does not solve any mysteries. It does not start where the above story stops and does not provide neatly packaged answers for governments, lawyers and businesses as to how to respond to the transnational Internet.[2] Its aim is simply to retell the story and make it comprehensible. The book sets out to map the legal landscape within which the Internet falls, focusing on its transnational nature; a map with a legend which allows the interested traveller to read and disentangle the legal web of the web; it sets out to explain the common themes running through seemingly discrete transnational problems and why some apparently similar transnational cases are fundamentally as distinct as a capital city from a big city. Finally, this book hopes to show the basic options open to regulators to remodel our legal landscape to suit the new online demands better, as well as the costs and benefits of those models.

Essentially, the discussion maps battlefields, wars fought on innumerable fronts. What all these scenes of conflict have in common is that they present a clash between the transnational Internet and national law. The law struggles with the global reach of the Internet, while everyone else revels in it. Being able so easily to cross borders and enter foreign places to chat, see, meet, do research, arrange, shop, sell, in short to conduct so many daily activities, means that the world has shrunk; the global village

[2] In this book, the term 'Internet' is generally used interchangeably with the World Wide Web, although this is strictly speaking incorrect. The focus of the book is generally on websites, although many of the arguments raised are also applicable – with some adaptation – to other Internet services such as email, chat rooms or discussion groups. Chapter 7 considers commercial email.

has more than ever become a reality.[3] Physical distance still matters, but far less so. The opportunities arising from this bottom-up globalisation are immense and exist on many levels, economic, cultural or political: some have been seized, such as trading opportunities, others need more time; for example, it has been argued that in the long term the Internet is likely to be a force for democracy even though authoritarian regimes appear capable in the short to medium term of halting its democratising effect.[4]

And yet, despite all these opportunities, or indeed because of them, in legal terms the global nature of the Internet is first and foremost problematic.[5] The reason is simple. Law and regulation have been organised on the assumption that activities are on the whole geographically delimited: the right to regulate conduct is shared out between geographically defined States on a predominantly geographic basis – each State can regulate what occurs within its territory. Location is the criterion for the sharing of activities. This basic allocation rule works well when conduct is generally located within a single territory. Then it is clear what belongs to whom. Yet online activity is not by default located in a single territory. *Prima facie*, a website can be accessed everywhere. Does this mean that every State can regulate every site and, if not, which State can and which State cannot? Where is the site located for the purposes of establishing which State can assert a regulatory right? Although regulators have for years struggled with rising transnationality, in the form of global trade and transnational corporations, the Internet presents an entirely new dimension to the problem of squeezing transnational activity into the national legal straitjacket.

So this book provides a map of these scenes of conflict, but what exactly is its scale? There is no doubt about it: it is a world map. This is true in a number of aspects. First, this book trades in ideas and generic arguments illustrated by reference to specific archetypal examples. No encyclopaedic account of all relevant legal developments is given or

[3] Marshall McLuhan tends to be credited with coining the phrase 'global village' in the 1960s (alternatively, P. Wyndham Lewis). It encapsulates the idea that the media recreates (and strive towards recreating) the village experience. This idea is well explored in Paul Levinson, *The Soft Edge – A Natural History and Future of the Information Revolution* (London: Routledge, 1997).

[4] Shanthi Kalathil and Taylor C. Boas, 'The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution' (2001) Carnegie Endowment Working Papers, Global Policy Program No. 21, www.carnegieendowment.org/files/21KalathilBoas.pdf.

[5] This is not to say that the Internet does not also provide governments, the law and lawyers with significant opportunities.

intended. The assumption is that the generic arguments and ideas can be applied to other instances, but listing all of them would be as tedious as it would be unnecessary. The aim is to allow the traveller to locate any specific points of inquiry within this wider legal map, but for a street plan of any particular city more specialised treatises need to be consulted. However, by explaining one or two cities, it is hoped it will become clear how cities are organised and the problems to which they give rise, at least in principle. The finer details are then child's play. Secondly, and interrelatedly, the discussion is not restricted to any one area of substantive law, cutting across private or civil law (such as contract, tort and intellectual property law) to various areas of public or criminal law (such as hate speech and gambling law). However, each chapter makes one of these substantive areas the trigger for the generic issues without excluding other areas. Despite contrary appearances, the focus is always narrow, not examining the substantive law, but merely asking the question in what circumstances is the law of a State applicable.[6] In what circumstances has a State the right to make, apply and enforce its contract or tort or criminal law in respect of online activity, and what happens when that right runs concurrently with the rights of other States?

Thirdly, not only does the inquiry extend over various substantive areas of law but it also shows no respect for national legal boundaries. The discussion freely crosses oceans, cultures and languages (as far as practicable) and examines comparable jurisprudence of the UK, the US, France, Germany, Canada and Australia. Indeed, if this book shows one thing, it is that we are all in this together, and not just in terms of being exposed to the same problem. States are hard pushed to realise their regulatory objectives without talking to each other; they can no longer pretend to be regulatory islands. Such talks in various forms are already well underway;[7] also in the online context, judges, legislators and academics now routinely take note of foreign legal developments. For such talks to be fruitful, there is a need for robustness with one's own

[6] In this context, 'law' includes both the substantive and procedural law of a State as well as its legal processes, such as adjudication or executive action.

[7] Of the enormous number of such 'talks', a high-profile example is the World Summit on the Information Society (an initiative of a UN agency, the International Telecommunications Union), www.wsis.org, which met for the second time in Tunis in 2005. An initiative arising from the summit was the creation of the multi-stakeholder Internet Governance Forum, www.intgovforum.org. A highly active international institution in this field is the Organization for Economic Co-operation and Development (OECD), www.oecd.org.

peculiarities, and a willingness to focus on the commonalities. In any event, in so far as the discussion concerns jurisdiction in respect of criminal and other public law, it is customary international law which provides the source of the legal rules in question. Thus, ascertaining how various States have responded to the same or similar transnational problems, far from being indulgent and unrestrained, is essential to establish the relevant State practice and *opinio juris*.[8] Yet, private international lawyers accustomed to dealing with one national system at a time, may feel ill at ease with the agility with which the discussion – any national peculiarities aside – jumps from one system to another.[9] By way of justification, I can only reiterate the above and add that it seems time that private international lawyers do their name justice and become more international.

In short, this book's ambition is nothing less than to provide a world map of the attempts of national legal systems to absorb the transnational online world, the problems associated with these attempts and actual and likely solutions.

C. *Who cares?*

So, does anyone really care? The sheer amount of literature on the topic generated by governments, professional and industry bodies[10] and international institutions (such as United Nations agencies,[11] the

[8] For an overview of the jurisdiction principles under customary international law, see Bernard H. Oxman, 'Jurisdiction of States', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987) Vol. 10, 277.

[9] By the same token, the discussion implicitly rejects the scepticism some have voiced in respect of comparative law and the ability to compare diverse legal solution given 'the difficulty of identifying similar legal issues in diverse societies and cultures': Peter Thomas Muchlinski, 'Globalisation and Legal Research' (2003) 37 *International Lawyer* 221, 227f. The discussion not only shows that many States face exactly the same Internet-related legal issues but also that the technical differences in national laws tend to mask similar underlying concerns and policy decisions.

[10] One of the most comprehensive general treaties on competence in the online environment is: American Bar Association, 'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf. Government reports tend to be on specific substantive topics, with competence issues being one of the issues considered; see, for example, UK Law Commission, *Defamation and the Internet – A Preliminary Investigation*, Scoping Study No. 2 (December 2002), www.lawcom.gov.uk/docs/defamation2.pdf.

[11] For example, the United Nations Commission on International Trade Law (UNCITRAL) focusing on the harmonisation of national law affecting e-commerce, www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html.

Organization for Economic Co-operation and Development,[12] the Hague Conference on Private International Law[13] and the World Trade Organization[14]) certainly suggests that the topic under consideration is not just of academic interest.[15]

The reason for its prominence lies first and foremost in the need to respond to real and immediate disputes arising out of online activity. The growth of online activity has been matched by a corresponding growth of transnational civil disputes – a trend which is likely to continue with the further growth of Internet presence: by the end of 2005 the worldwide Internet population was estimated to be 1.08 billion and is projected to almost double by 2010.[16] Apart from private disputes, governments too are under real pressure to deal with online

[12] The OECD has produced a vast amount of literature on various transnational aspects of e-commerce and Internet governance generally. See, for example, OECD, *OECD Input to the United Nations Working Group on Internet Governance (WGIG)* (2005) DSTI/ICCP(2005)4/FINAL, www.oecd.org/dataoecd/34/9/34727842.pdf; OECD, *The Use of Authentication Across Borders in OECD Countries* (2005) DSTI/ICCP/REG(2005)4/FINAL, www.oecd.org/dataoecd/1/10/35809749.pdf; OECD, *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (2003), www.oecd.org/dataoecd/24/33/2956464.pdf; and *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2002).

[13] Hague Conference on Private International Law (Andrea Schulz, ed.), *Proceedings of the International Conference on the Legal Aspect of an E-Commerce Transaction 2004*, http://hcch.e-vision.nl/index_en.php?act=progress.listing&cat=9/.

[14] See, for example, World Trade Organization (WTO), *Electronic Commerce and the Role of the WTO*, Special Study 2 (1998), www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf.

[15] The amount of academic literature on the topic of competence is enormous. Some of the more comprehensive treatises are: Adam Thierer, and Clyde Wayne Crews Jr (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: Cato Institute, 2003); Henricus Snijders and Stephen Weatherill (eds.), *E-Commerce Law: National and Transnational Topics and Perspectives* (The Hague: Kluwer Law International, 2003); Paul Schiff Berman, 'The Globalisation of Jurisdiction' (2002) 151 *University of Pennsylvania Law Review* 311; Karsten Bremer, *Strafbare Internet-Inhalte in International Hinsicht – Ist der Nationalstaat wirklich überholt?* (Frankfurt a. M.: Peter Lang Verlag, 2001), http://ub-dok.uni-trier.de/diss/diss60/20000927/20000927.pdf; Bradford L. Smith, 'The Third Industrial Revolution: Law and Policy for the Internet' (2000) 282 *Recueil des Cours* 229 (a more general discussion of Internet governance which also addresses competence issues); and a special edition on jurisdiction in *The International Lawyer* (Vol. 32, 1998).

[16] See ClickZ, *Population Explosion*! (3 November 2005), www.clickz.com/stats/sectors/geographics/article.php/5911_151151. Note that, by the end of 2002, an estimated 655 million people worldwide were using the Internet. United Nations Conference on Trade and Development (UNCTAD), *E-Commerce and Development Report 2002* (2002) UNCTAD/SDTE/ECB/2. For more recent world statistics on Internet usage, see OECD, *OECD Input to the United Nations Working Group on Internet*

activity, to protect children from unsuitable websites and to protect local, legally compliant businesses from unfair online competitors, and, to those pressure groups, it matters little whether the online activities come from abroad or not. So these are tangible and immediate needs that the general debate on regulatory competence addresses and into which this book taps.

More generally, there can be no doubt that finding solutions to competence issues is pivotal to maintaining law and order: 'There is no more important way to avoid conflict than by providing clear norms as to which state can exercise authority over whom, and in what circumstances. Without that allocation of competence, all is rancour and chaos.'[17]

If it is not clear who is in charge of a particular situation or activity (if too many or too few take it upon themselves to get involved), the situation or activity is unlikely to be effectively regulated. So an inadequate system for allocating regulatory responsibility undermines the effectiveness of substantive laws, which is the underlying worry. And such ineffectiveness is not neatly restricted to the online space. A failure to regulate the Internet effectively undermines the credibility and effectiveness of the regulation of equivalent offline activity. What is the point of, and how can you justify, a prohibition of physical gambling operations, if similar online gambling operations are beyond the regulatory reach? Does it make sense to insist on a prescription for a drug if that same drug can be bought freely online, and, if so, why?

This leads directly to a further concern on a perhaps more distant but no less serious level: currently, the whole system of allocating regulatory competence and the territoriality principle are deeply embedded in the notion of statehood. Control over a State's territory is not just a consequence of statehood but also an essential attribute:[18] having a territory and control over it is part of what it means to be a State. The colour of eggs did not just provide the criterion for allocating eggs

Governance (WGIG) (2005) DSTI/ICCP (2005)4/FINAL, www.oecd.org/dataoecd/34/9/34727842.pdf.

[17] Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon, 1994), 56.

[18] Helmut Steinberger, 'Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 397, 413, where the author notes: 'Exclusivity of jurisdiction of States over their respective territories is a central attribute of sovereignty.' Note that a delimited territory is an element of statehood; see Art. 1 of the Montevideo Convention on Rights and Duties of States (1933) and e.g. Jochen Frowein, 'Recognition', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 340, 341: 'the recognition of States presupposes the existence of the criteria for statehood, i.e. a fixed territory, a population and an effective government.'

but defined the egg industries as such. Take away the colour and you take away the *raison d'être* of the industries in their various shapes and sizes. Similarly, as the Internet undermines the criterion of territoriality as a basis for sharing regulation,[19] it chips away at the State itself; the State which is the territorially defined and territorially empowered regulatory institution. As the notion of statehood is so elementary to our understanding of law and indeed life in general, it is hard to envision either without the State.[20] It is also counterintuitive to see the State not simply as an institution subject to the territoriality principle but as its very personification. But that is what it is. How tightly the notion of regulatory power, territoriality and statehood are interwoven shines through the words of Mann: 'International jurisdiction is an aspect or an *ingredient* or a consequence of sovereignty (or of territoriality or of the principle of non-intervention – the difference is merely terminological).'[21] When Mann uses 'sovereignty' interchangeably with 'territoriality' and the 'principle of non-intervention', he could also have referred to the sovereign territorial State.

With online events it is harder than ever to say with ease and certainty that 'this is yours and this is mine'. But, even when that is decided, States often lack the actual power to impose their will on those sites which relentlessly penetrate their borders. While States have a theoretical entitlement to 'control' what happens on their territory, they often lack the practical means to do so.[22] This has prompted some to argue that, long-term, the State is not viable. However, the State has proved rather hardy in respect of previous challenges such as the rise of transnational corporations; the Internet is not the first phenomenon to

[19] David R. Johnson and David Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367; Henry H. Perritt, 'Cyberspace and State Sovereignty' (1997) 3 *Journal of International Legal Studies* 155; Henry H. Perritt, 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance' (1998) 5 *Indiana Journal of Global Legal Studies* 423; Jack L. Goldsmith, 'The Internet and the Abiding Significance of Territorial Sovereignty' (1998) 5 *Indiana Journal of Global Legal Studies* 475.

[20] Although within legal and political scholarship 'the contingency of the nation state' has long been recognised: Berman, above n. 15, 321, 441ff; more generally see, for example, Günther Teubner, *Global Law without a State* (Aldershot: Dartmouth, 1997).

[21] F. A. Mann, 'The Doctrine of International Jurisdiction Revisited After Twenty Years' (1984) 186 *Recueil des Cours* 9, 20 (emphasis added). See also F. A. Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recueil des Cours* 1, reproduced in F. A. Mann, *Studies in International Law* (Oxford: Clarendon Press, 1973). Generally on sovereignty, see Steinberger, above n. 18.

[22] This relates to enforcement jurisdiction: see below and Chapter 6.

undermine State control over its territory[23] and trigger a prognosis of doom for the State. '[S]overeignty over territory will disappear as a category from the theory of international society and from its international law . . . [I]nternational society will find itself liberated at last to contemplate the possibility of delegating powers of governance not solely by reference to an area of the earth surface.'[24]

So far, these predictions have not been realised,[25] and so perhaps equal sentiments about the demise of the State expressed in relation to the online world need to be treated with caution:

> The Internet has neither changed the central position of the nation state in world politics nor the classic power games. Yet, it further strengthens existing restrictions on the possible actions of nations and promotes the creation of a global civil society. Both will in the long term affect the position and actions of the nation state. It is not going to disappear, but it will change . . . The Internet, like the invention of the printing press, is likely to deeply change culture, society and politics, yet its long-term effects are as unpredictable as the effects of the printing press at the time of the first books.[26]

What form, if any, the State will take long-term is largely speculative and will not be further discussed here. Nevertheless, one positive practical effect of abandoning the notion of statehood as a *sine qua non* without which law could not possibly function, is that it frees the debate on

[23] Again, there is a vast literature on this topic in various contexts. For one example, see Robert McCorquodale and Raul Pangalangan, 'Pushing Back the Limitations of Territorial Boundaries' (2001) 12 *European Journal of International Law* 867, 879: '[T]he exclusive territorial sovereign power of the state is being diminished and states are increasingly being shown to be unable to control the activities of transnational corporations.'

[24] Philip Allott, *Eunomia: A New Order for a New World* (Oxford: Oxford University Press, 1990), 329.

[25] Although there are some who argue that the sovereign State is already in the process of significant transformation. See, for example, Christopher Harding, 'Legal Subjectivity as a Fundamental Value: The Emergence of Non-State Actors in Europe', in Kim Economides *et al.* (eds.), *Fundamental Values* (Oxford: Hart Publishing, 2000), 115; cf. Peter Thomas Muchlinski, 'Globalisation and Legal Research' (2003) 37 *International Lawyer* 221 (where the author, although acknowledging various legal globalisation trends, cautions against overestimating the impact of supranational law).

[26] Karl Kaiser, 'Wie das Internet die Weltpolitik verändert' (2001) 3 *Deutschland – Zeitschrift fuer Politik, Kultur, Wirtschaft und Wissenschaft* 40, 45 (translation by the author). See also Saskia Sassen, 'The Impact of the Internet on Sovereignty: Unfounded and Real Worries', in Christoph Engel and Kenneth H. Keller (eds.), *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values* (Baden-Baden: Nomos, 2000), 195, www.mpp-rdg.mpg.de/pdf_dat/sassen.pdf.

solutions to the legal quagmire of the Internet and opens it up to less State-centric ideas. That cannot be a bad thing.

D. A conservative approach

Having said that, the problem in the past has not been that the legal debate on competence and the Internet has been too State-centric but rather that it has not been State-centric enough. Especially in the early days of the online revolution in the mid-1990s,[27] many legal academics were all too ready to discard traditional state-based laws as capable of ordering the online world. Two of the more high-profile ones were Johnson and Post, who, in their article, 'Law and Borders – The Rise of Law in Cyberspace',[28] argued that '[g]lobal computer-based communications cut across territorial borders ... undermining the feasibility – and legitimacy – of laws based on geographic boundaries'.[29] Their central assertion was that the traditional jurisdictional rules based on geographic location are not transferable to the transnational Internet. They concluded that cyberspace should be treated as a distinct and independent place for regulatory purposes.[30] The idea had appeal, initially even to governments:

> The idea that cyberspace should be presumptively self-governing has resounded in thoughtful scholarship. It has also colored federal policy regarding electronic commerce. A 1997 Presidential Directive, which heralded the dramatic withdrawal of the United States government from significant portions of Internet administration, instructs federal agencies to 'recognize the unique qualities of the Internet, including its decentralised nature and its tradition of bottom-up governance'.[31]

Yet, the legal developments which have taken place since then are a far cry from Johnson and Post's assertion and prediction, with States now consistently applying traditional territorially based rules to online activity and largely refusing to treat the Internet as beyond their

[27] When the Internet took off on a popular and commercial level.

[28] Above n. 19. [29] Above n. 19, 1367.

[30] Above n. 19, 1378, where the authors argue that '[m]any of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world".'

[31] Neil Weinstock Netanel, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 *California Law Review* 395, 398 (footnotes omitted).

competence.[32] The debate has moved on from the question of *whether* States should regulate the transnational Internet to the question of *how* it can be done. Despite these early predictions being proved wrong, they do raise interesting questions as to how law changes in response to new phenomena, why the most obvious, rational and effective legal solutions do not necessarily carry the day and what the implications of chosen second-rate solutions are. These questions are explored in Chapters 2 to 4 of this book, which show how basic law concepts such as *stare decisis*, formal justice, the rule of law and foreseeability of legal obligations continue to play a vital role in defining the problems at hand and circumscribing the range of potential solutions. Furthermore, they also highlight the danger of culturally isolated legal thinking in a globally connected world.

The argument throughout this book is conservative, relying on past decisions, concepts, legal structures and traditions to evaluate present problems. It employs 'a restrained, relatively apolitical method of analysis ... [which] combines two characteristics: the willingness to work from the institutionally defined materials of a given collective tradition and the claim to speak authoritatively within this tradition'.[33] This approach builds upon the belief that legal doctrines display 'impersonal purposes, policies, and principles'[34] – the recognition of which is capable of yielding realistic legal solutions, unlike the 'open-ended disputes about the basic terms of social life, disputes that people call ideological, philosophical, or visionary'.[35] Based upon similar considerations, the discussion does not go into issues which have surfaced in more multidisciplinary papers on competence and governance, such as space, identity, distance and community.[36]

Yet, whatever the advantages of this sober, relatively black-letter-law approach, it creates a danger, as illustrated by the egg story. Submerging

[32] This applies particularly to adjudicative and legislative jurisdiction: see below and Chapters 2 to 5.

[33] Roberto Unger, 'Critical Legal Studies Movement' (1983) 96 *Harvard Law Review* 561, 565 (defining legal formalism) and 564: 'the distinctive rationality of law is imminent in the legal material on which it operates ... [and] is characterized by the working out of implications of law from a standpoint internal to law.' See also Ernest J. Weinrib, *The Idea of Private Law* (Cambridge, MA: Harvard University Press, 1995), 22f, where the author defends legal formalism as embodying 'a profound and inescapable truth about law's inner coherence'.

[34] Unger, *ibid*. [35] Unger, *ibid*.

[36] A classic example is Berman, above n. 15; Will Taggart, 'The Digital Revolt: Resistance and Agency on the Net' (2001) *New Media and Information Technology in the Middle East*, http://nmit.georgetown.edu/papers/wtaggert.htm.

oneself within the very legal rules which are problematic means that it is easy to lose sight of the wider picture, the broader implications of the rules as well as of the legal framework: 'the individual . . . become[s] so absorbed in the narrow technical aspect of the task that he loses sight of its broader consequences. The film *Dr Strangelove* brilliantly satirized the absorption of a bomber crew in the exacting technical procedure of dropping nuclear weapons on a country.'[37] Given the complex and technical nature of the allocation rules particularly in private matters, this is a real danger. The discussion here (as presumably with every academic treatise) tries not to succumb to this danger but cannot be entirely immune to it; also, ultimately, defining what is the wood, and what are just trees, is of course the main point of contention.

Finally, given this book's preoccupation with law and technology, a brief comment is called for on the commonly held view that legal discussions of new technological phenomena require a deep understanding and analysis of the technical processes underlying the phenomenon and that these technicalities are in some ways determinative of the legal questions. The discussion here is based upon a rejection of both assumptions, and implicitly defends the idea that it is not the technical processes *per se* which are legally decisive[38] but their effects. For example, it *is* highly relevant to the legal debate on competence whether website operators can through technical measures limit the reach of their sites to certain territories and how reliable and effective these measures are. However, what the exact technical processes underlying such capability are is of little interest to the lawyer and firmly belongs in the technician's laboratory.

2. The building blocks

A. Jurisdiction

The central building block of this book is the concept of jurisdiction – a term which has so far been carefully avoided out of fear of alienating

[37] Stanley Milgram, *Obedience to Authority* (London: Tavistock, 1974), 7.

[38] For some support for this view, see, for example, *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305, paras. 14f: 'The affidavit . . . attempted to trespass on to the area of the legal conclusion as to how and when, for the purposes of the law of defamation in relation to the Internet, publication took place . . . [They] are illuminating . . . in addressing the technical process whereby a document finds its way from one computer to another via the World Wide Web . . . However, the appreciation of . . . the technologies . . . cannot dominate the question of publication for the law of defamation.'

private and public international lawyers alike, even before the story unfolds. Yet, because this book breaks with convention and examines 'jurisdiction' in both private and public matters, it is critical to explain its usage here. 'Jurisdiction' derives from the Latin *juris dictio*, meaning the 'administration of justice'.[39] In Roman times, it acquired the meaning with which it tends to be associated today, namely, the legal power, right or authority to regulate. In the purely domestic context, this usually refers to the right or competence of one State organ (such as a court) *vis-à-vis* another one (such as the executive) to take action in respect of a particular matter, as defined by constitutional law. This book is not concerned with this meaning of 'jurisdiction'.

The discussion concerns 'jurisdiction' only in the transnational context. But even there the term connotes different things depending on the context. First, in its broadest sense, it refers to the regulatory competence or power of a State *vis-à-vis* other States: the right to regulate. Jurisdictional rules in this broadest sense are about the sharing of regulatory space between States, about the '*juste partage de souveraineté*'.[40] Secondly, sometimes, it is also used to refer to the physical territory of a State.[41] So it is no tautology to say that a State has jurisdiction (the right to regulate) within its jurisdiction (on its territory) and sometimes over matters outside it. Thirdly, private international lawyers use the term much more narrowly, referring to the issue whether a court has the right to hear a transnational dispute. While this book uses the term in all three senses, most commonly it will be used in its widest sense, i.e. the power or right to regulate,[42] and from the context it should be clear when a more narrow meaning is envisaged.

A State may exercise its regulatory power through its judiciary or its legislature or its executive. For the private international lawyer, referring to the State as assuming any kind of jurisdiction is rather inaccurate as the State as such has no or very limited interest in the dispute and gets

[39] Ivan Shearer, 'Jurisdiction', in Sam Blay, Ryszard Piotrowicz and Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005), 154, 154.

[40] Mann (1964), above n. 21, 18. This though does not mean that other States do not enjoy concurrent regulatory competence, as discussed below.

[41] For the varying meanings of 'jurisdiction', see also *Lipohar* v. *R* (1999) 168 ALR 8, paras. 78f.

[42] The rules of jurisdiction, while *prima facie* always in operation, only become interesting when a matter is transnational, i.e. not of purely domestic concern. Domestic matters are not subject to international law (bar some exceptions) but of course it is international law which defines what is and is not a domestic matter.

involved at most only as a facilitator.[43] Consequently, they tend to adopt more neutral language in which the *legal system* prescribes the rules and *the courts* adjudicate the dispute. Such neutral language is not always adopted here, without any strong intention to challenge this view of the State's limited involvement in private matters,[44] but mainly for the convenience of adopting comparable language for both private and public law.

The rules which determine competence are jurisdictional rules. A jurisdictional rule is 'an odd creature among laws. It never tells what the result will be, but only where to look to find the result.'[45] Jurisdictional rules lay down what nexus is needed between the State and the activity or person to be regulated to found an entitlement to regulate. What these rules are and where they can be found depends broadly on two matters. First, it depends on the private/civil or public/criminal nature of the dispute. If the dispute or matter is private, it is private international law[46] and if it is public it is public international law which provides the legal source. However, it is rare for courts, at least within the common law tradition, to refer explicitly to public international law

[43] This view is implicitly also reflected in public international law, which is said to govern the relationships of States but held by most to impose no limitations or restrictions on private international law, presumably because this area of law is perceived as not concerning the relationship between States. See below n. 46.

[44] Generally, this book treats states within a federation, such as the US or Australia, like independent States, but is conscious of the fact that at times decisions on disputes involving states within a federation are guided by considerations which are inapplicable in the truly transnational context, and *vice versa*. See, for example, §10 of the US Restatement (Second) of Conflict of Laws (1971) and Comments. This applies both in the civil as well as in the criminal context; see eg. *Regie National des Usines Renault SA* v. *Zhang* [2002] HCA 10 and *Lipohar* v. *R* (1999) 168 ALR 8, paras. 99f.

[45] Brainerd Currie, *Selected Essays in the Conflict of Laws* (Cambridge: Cambridge University Press, 1963), 170.

[46] Every State has its own rules of private international law which are highly technical and vary widely. For the EU, see, for example, Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations (Rome II), COM(2003) 427 final, 5f. Thanks to the efforts of the Hague Conference on Private International Law, there are quite a few treaties which harmonise private international law and make it part of public international law. Public international law is generally (but not always) considered not to impose any limitations upon private international law. Gerfried Mutz, 'Private International Law', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 330, 334, where the author argues that public international law does not require States to have any private international law system. Michael Akehurst, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145, 177. For a contrary view, see Shearer, above n. 39, 158.

in prosecutions concerning transnational criminal activity. Instead, they rely on domestic doctrines and constructs (as, for example, 'all crime is local') to explain why a local prosecution would or would not be legitimate.[47] Although there is disagreement as to whether such constructs ultimately derive their authority from public international law,[48] it is widely accepted that they have to be consistent with it. In short, public international law governs extra-territorial criminal jurisdiction.

Secondly, jurisdiction also varies depending on the regulatory act which a State seeks to assert. Regulatory activity in the transnational legal context tends to be divided into three types: the right to prescribe laws,[49] the right to adjudicate disputes and the right to enforce the rules or judgment. Only within its territory has a State full jurisdiction, that is all three types. While in some circumstances a State may prescribe laws and adjudicate disputes in respect of persons or matters outside its territory, its enforcement jurisdiction does not reach beyond its territory. In other words, adjudicative and legislative jurisdiction have an extra-territorial reach, but a State can never send its police or other agents into another State's territory to enforce these claims.

This three-part division of regulatory activity is reflected in transnational private disputes where one State (i.e. legal system) may prescribe the law, but another may adjudicate and enforce it. In respect of public or criminal matters, there is no choice of law: once a State assumes adjudicative jurisdiction over a person, the court will always apply forum law, i.e. never foreign law, and thus adjudicative and prescriptive jurisdiction collapse for most intents and purposes into one.

This systematisation is rather uncontroversial as far as private law is concerned. The same, however, cannot be said for public law, where

[47] See, for example, Matthew Goode, 'The Tortured Tale of Criminal Jurisdiction' (1997) 21 *Melbourne University Law Review* 411.

[48] In other words, there are divergent opinions on whether States derive their competence from public international law or whether they have competence by virtue of their sovereignty (which precedes rather than derives from international law) and public international law merely imposes limitations on that 'natural' competence States possess. This debate dates back to the decision of the Permanent Court of International Justice in *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No. 10, 20, where the Court favoured the latter view: 'Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property, and acts outside their territory, it leaves them in this respect a wide measure of discretion which is only limited in certain cases by prohibitive rules.'

[49] This applies to both judge-made law and legislation.

Table 1 *Overview of regulatory competence*

	Adjudicative jurisdiction Also referred to as judicial jurisdiction, jurisdiction of the courts, curial jurisdiction	**Prescriptive jurisdiction** Also referred to as subject-matter jurisdiction, legislative jurisdiction	**Enforcement jurisdiction** Also referred to as executive jurisdiction
Private law governed by each State's private international law (conflict of laws[a])	E.g. jurisdiction *in rem* or *in personam* Basis of jurisdiction e.g. service of writ within the jurisdiction	Choice of law (i.e. court may apply foreign substantive law) Bases of jurisdiction e.g. location of the tort, contractual choice, place of the contract	Basis of jurisdiction: strictly territorial (but agreements for the reciprocal enforcement of foreign judgments)
Public law governed by the jurisdiction rules of public international law	A court which assumes jurisdiction always applies its own law (no choice of law). Bases of jurisdiction: territoriality principle, nationality principle, universality principle, protective principle, passive personality principle[b]		Basis of jurisdiction: strictly territorial (no enforcement of foreign judgments)

Notes:

[a] In this book, the terms 'private international law' and 'conflict of laws' are used interchangeably, although this practice is not universally supported: Mutz, above n. 46, 331.

[b] Note that some discuss these bases under the heading of prescriptive jurisdiction and others under adjudicative jurisdiction. As it generally does not matter whether a State asserts excessive extraterritorial jurisdiction merely in a statute without taking any further action, it would appear that the bases of jurisdiction are logically discussed under adjudicative jurisdiction when the first step towards enforcement is taken. Having said that, the mere claim of regulatory competence in a statute is not entirely harmless as it may give rise to defensive actions by, for example, companies or other actors. Shearer, above n. 39, 156.

there is disagreement as to the appropriate systematisation. For example, Mann categorises adjudicative jurisdiction as a sub-category of enforcement jurisdiction.[50] This is logical in so far as adjudicative jurisdiction is exercised to enforce a law. Yet, it seems inconsistent with the general understanding of enforcement jurisdiction as the power finally to give effect to a rule or judgment through the imposition of consequences such as the loss of liberty or property. For this reason, the above systematisation follows what is possibly the more commonly held view of international jurisdiction, distinguishing between the three types of jurisdiction,[51] while acknowledging that adjudicative and legislative jurisdiction overlap (as there is no choice of law).[52] This has the added advantage of better enabling a comparison to be drawn to private international law. It is also justifiable given that the difference in the systematisation is often of no more than academic interest. Even international lawyers who view adjudicative jurisdiction as part of enforcement jurisdiction hold that the 'assumption of the power to adjudicate a dispute . . . may be judged by the same principles as are applicable to an exercise of legislative (prescriptive) jurisdiction'.[53] Last but not least, enforcement jurisdiction is clearly distinct. It is the Achilles' Heel: whatever regulatory claims they may try or would like to assert under adjudicative or prescriptive jurisdiction, enforcement jurisdiction puts a stop to many of them. (But more on that later.)

[50] F. A. Mann, *Studies in International Law* (Oxford: Clarendon Press, 1973), 128. He appears to have revised his opinion later in Mann (1984), above n. 21, 67: 'The international jurisdiction to adjudicate is . . . not a separate type of jurisdiction, but merely an emanation of the international jurisdiction to legislate.' See also Shearer, above n. 39, 157. See also Luc Reydams, *Universal Jurisdiction – International and Municipal Legal Perspectives* (Oxford: Oxford University Press, 2003), 25: 'Most popular are the three-pronged distinction between legislative, judicial, and executive jurisdiction (by reference to the three traditional branches of State authority) and the two-pronged distinction between prescriptive and enforcement jurisdiction (by reference to the substance of the powers exercised)' (footnotes omitted). Generally, see also UK Home Office, *Review of Extra-Territorial Jurisdiction*, Steering Committee Report (1996).

[51] Akehurst, above n. 46; Oxman, above n. 8, 277f. See also §§402–33 of the US Restatement (Third) of Foreign Relations Law (1986).

[52] Note that, in US jurisprudence, these two areas are treated separately: see Part IV of the US Restatement (Third) of Foreign Relations Law (1986). Such distinctions are not adopted elsewhere. For example, in England and Australia, it is assumed that a court has personal jurisdiction 'over the body of the person found within its territory. It is another question whether that authority will assume "jurisdiction" over the *legal subject-matter* with which that person is concerned.' Goode, above n. 47, 412 (footnotes omitted, emphasis in the original). Generally, prosecutions are not commenced *in absentia*.

[53] Shearer, above n. 39, 167; Mann (1973), above n. 50, 128f.

B. Public law versus private law

As noted above, this book departs from the general tendency to see competence issues in respect of public law and private law as two strictly separate subjects which defy discussion under one heading.[54] This heresy is based upon my firm conviction that the initial legal issues in both scenarios are virtually indistinguishable and that comparing the different approaches taken to them yields insights into the nature of public and private law, into the strengths and weaknesses of both sets of jurisdictional rules, and into the relationship of States with each other more generally.

As the discussion seeks to transcend the particular competence rules of the discrete areas of substantive law such as torts or contract, what emerges are the generic competence problems to which the Internet gives rise. Also, similarities of the legal responses within the broader public-law and private-law categories become apparent; and this has practical significance. It shows that reliance on jurisprudence derived from other subject-matters within the same category is legitimate and often fruitful. By the same token, given the deep-seated differences between the responses to jurisdictional problems in private and public law, cross-referencing between these broader categories needs to be treated with extreme caution. The insights gained from this comparison should be of interest beyond the online context.

This undertaking requires an understanding of the meaning of private law and public law. Initially, the distinction appears rather obvious, but – as will be seen in Chapter 6 – on closer analysis these are rather slippery concepts.[55] At this stage, suffice it to say: 'public law' is used to refer to criminal, administrative, revenue and generally regulatory law.[56] It refers to those obligations on the individual imposed and enforced by the State itself as a matter of prerogative. 'Private law' and 'civil law' are used interchangeably, referring to those obligations which private persons owe to, and enforce against, each other, such as obligations arising under contract, tort law or intellectual property law.

[54] For notable exceptions, see Akehurst, above n. 46, and Mann (1964) and (1984), above n. 21.

[55] Oxman, above n. 8, 278.

[56] Sir Robert Jennings and Sir Arthur Watts (eds.), *Oppenheim's International Law* (9th edn, London: Longman, 1992), Vol. 1, 466 (n. 3), 473 (n. 39).

C. *The quest for the perfect link*

The law on transnational competence is concerned with the allocation or sharing of regulatory responsibility between States. It embodies the view that law and order across the globe are best achieved if divided up[57] and each actor has a clearly demarcated parcel of competence. The competence rules are designed to isolate the 'worthiest' State (or legal system), the one most closely connected to the facts of the case. Often they turn a blind eye to the fact that an event is transnational and ideally make one State, rather than all those affected, legally responsible for it.

In the egg story, that link to show entitlement was colour. In the real world, the types of link required are myriad, based on a variety of factors, as discussed above. Nevertheless, despite these variations, there is one denominator which is common to most of them and that denominator is location: the location of the conduct, the parties or the property.[58] In public international law, it is the territoriality principle – the primary basis of jurisdiction – which makes the location of the conduct or person the explicit touchstone of the regulatory right.[59] In private law, the location of the defendant, the location of the tort or of the contractual agreement or of the registration of the patent or trademark are all instances of location-focused links. There are exceptions. The nationality or universality principles are such exceptions in public international law.[60] The former takes the nationality of the offender as the justifying link and the latter dispenses altogether with the need for a link in relation to certain heinous acts that threaten the international

[57] The concept of the common heritage of mankind, an example of which is the high seas, is an exception to the general division of competence. See Oxman, above n. 8, 278, generally on the objectives of competence rules in international law, and, for example, §6 of the US Restatement (Second) of Conflict of Laws (1971) and its comments on the purpose of choice of law principles.

[58] This may be tangible or intangible property such as intellectual property.

[59] Some have gone further and argued that territoriality also underlies those links which seem to be exceptions to it, such as the nationality principle. See e.g. Michael Byers, *Custom, Power and the Power of Rules* (Cambridge: Cambridge University Press, 1999), 64: 'the interests of a State in exercising jurisdiction are usually rooted in its territorial self. This enables States, when seeking to justify specific assertions of jurisdiction through constructive extensions of that principle, to act within an accepted conceptual framework of legality.'

[60] But note *ibid*.

community as a whole.[61] An example of a non-location-focused link in private international law is contractual choice: here the link with a legal system is created through the choice made by the contractual parties. But exceptions they are; exceptions to a world ordered by location-centric legal concepts. And, as will be seen, transplanting these location-centric links to online activities is fraught with difficulties.

In this context, another observation about these links needs to be made: both under public and private international law concurrent links have long been acceptable. And, indeed, in relation to most traditional transnational activity, it has always been likely that a number of States or courts could show a valid link and thus have a *prima facie* regulatory right. In public international law, this is, for example, because there are other bases of jurisdiction apart from, and running parallel to, territoriality.[62] In respect of private law, concurrent links result partly accidentally because of the lack of harmonisation of the rules allocating competence.[63] But they also exist by design; for example, the rules allocating which court can hear a dispute envisage the possibility of a number of competent courts, with additional remedial rules addressing conflicts should concurrent litigation actually occur.[64] Yet, despite the

[61] Akehurst, above n. 46, 162: 'Hijacking threatens international communications to the same extent as piracy; it is an attack on international order and injures the international community as a whole, which means that all States have a legitimate interest in repressing it.' Under most versions of the universality principle, the offender needs to be within the territory of the prosecuting States. For the different views of how the universality principle has been understood, see Reydams, above n 50, 288ff.

[62] Even territoriality by itself leads frequently (and in the online context invariably) to concurrent jurisdiction, as discussed below. But see, for example, Mann (1964), above n. 21, 50f: 'it would no doubt be desirable if the principle of exclusivity would come to be accepted for the purpose of jurisdiction, if, in other words, by common consent jurisdiction in respect of a given set of acts were exercised by one State only.' Akehurst, above n. 46, 192, where he comments in the context of global restrictive business practices that the number of States claiming jurisdiction should be as small as possible. For a defence of concurrent regulation in respect of public matters, see William S. Dodge, 'Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism' (1998) 39 *Harvard International Law Journal* 101.

[63] So different States may have different rules, for example, on the applicable law in tort or contract cases, with the result that, depending on where the action is brought, different laws would be applied to the same case – a problem which is partly redressed by the concept of *renvoi*.

[64] Once proceedings have started in one forum, doctrines such as *lis alibi pendens* (in civil law countries) or *forum non conveniens* (in common law countries) or the availability of anti-suit injunctions have developed to prevent concurrent jurisdiction. See e.g. Australian Law Reform Commission, *Legal Risk in International Transactions*, Report No. 80 (1996), paras. 6.55–6.57. However, the rules of jurisdiction under public

relative tolerance towards concurrent links, they need to be treated with caution. Just because concurrency has been acceptable does not mean that it is always a good thing. Sometimes it is: for example, when the law is relatively harmonised, concurrent competence helps to ensure that a wrongdoer does not slip through the net, no matter where he is located.[65] However, concurrent claims can give rise to too great a regulatory burden,[66] thereby making legal compliance difficult or even impossible and thus being rather counter-productive in terms of ensuring the effectiveness of all those concurrent laws. Finally, just because the law has lived quite comfortably with concurrent claims by two or three States in relation to a single transnational event does not mean that concurrent claims by hundreds of States over a single online event is equally acceptable.

Concurrency is an acute problem in the online context, where a multitude of States regularly claim (or would, if asked) the right to regulate the same website. Those rights are not infrequently asserted on the (territorial) basis that the website can be accessed in the State (which is true for most States). The vice as well as the virtue is that States can often not enforce these claims: it is a vice because it undermines legitimate regulatory attempts by States and discredits their unforceable laws; a virtue because it protects online participants from excessive regulatory burdens, as well as online content from being subjected to the most stringent legal standards worldwide.

international law deal poorly with concurrent and conflicting claims which are often resolved by the strict territorial limits of enforcement jurisdiction. Oxman, above n. 8, 282. See also David J. Harris, *Cases and Materials on International Law* (5th edn, London: Sweet & Maxwell, 1998), 265, stating that custody of a person tends to be decisive in resolving conflicting claims. The same sentiment is echoed in G. Fitzmaurice, 'The General Principles of International Law Considered from the Standpoint of the Rule of Law' (1957) 92 *Recueil des Cours* 209. But see also Jennings and Watts, above n. 56, 457 ('Usually the coexistence of overlapping jurisdiction is acceptable and convenient; forbearance by states in the exercise of their jurisdictional powers avoids conflict in all but a small (although important) minority of cases') and Mann (1964), above n. 21, 48 ('international lawyers know that the remedy again lies in a policy of tolerance, reasonableness and good faith').

With respect to concurrent criminal jurisdiction in the EU, see European Commission, *Green Paper on Conflicts of Jurisdiction and the Principle of Ne Bis in Idem in Criminal Proceedings*, COM(2005) 696 final.

[65] The universality principle ensures that, in respect of certain particularly heinous crimes which are condemned universally, every State has jurisdiction to prosecute the offender regardless of whether the offence was committed on that State's territory. See also above n. 62.

[66] See, for example, Oxman, above n. 8, 278. This is also to some extent reflected in the emerging *non bis in idem* principle in the EC: see Christine van den Wyngaert and Guy Stessens, 'The International Non Bis in Idem Principle: Resolving Some of the Unanswered Questions' (1999) 48 *International and Comparative Law Quarterly* 779.

One reason for this at least theoretical overregulation of online activity lies in the failure to adjust traditional legally accepted links in light of the new environment. The validity of a link (or claim) cannot be static but must always be *relative* to the strength of possible competing links (or claims). The law needs to look not merely for a link or connection *per se*, but at what is a close link in the context. 'Close links' cannot by definition be links all or most States could show. If that is the case, the link needs to be modified to be capable again of isolating the worthiest claimant(s). In other words, in an interconnected world, an entitling link must be a compromise between, on the one hand, the interests of States (and their subjects) in regulating transnational activity affecting them and, on the other hand, the need to limit the number of States asserting a regulatory right over the same activity.

In private international law, where justifying links are embodied in often long-settled and well-accepted tests provided for by statute or case law, it is easy to forget those overriding objectives, to see links in isolation rather than in their relative standing, and in such isolation they often seem perfectly legitimate but, as will be seen, this is deceptively so. In public international law, which does not enjoy the smug certainty of domestic law, the bases of jurisdiction are less hard and fast tests, more guidelines in a process informed by a higher consciousness of the overall picture: '[T]he principles rest on and are the typical results of a balancing of sovereignty between States and prohibited interference with internal affairs. As such, they make easier the difficult balancing task of legislatures and courts in a specific case: for legislatures the principles function as "signposts" when defining the scope ... of a norm, for courts they function as standardized balancing devices.'[67] Although the absence of strict tests creates less certainty, it should produce more balanced results. In principle, it should pre-empt the danger of too weak links being endorsed in relation to criminal online activity. But, as will be seen, the nature of criminal law is such that States almost invariably rely on weak links to justify their competence over foreign online activity.

This book explores the obstacles to a proper re-evaluation of traditional links in the online environment and, more importantly, the feasibility and the legitimacy of proposed links. The search is not for the perfect timeless link which is going to make all States happy ever after, for the simple reason that no such link can conceivably exist.

[67] Reydams, above n. 50, 23f (internal footnotes omitted).

In a globally interconnected world organised around location-centric principles, for entitling links to do their job well, there must be losers.

3. Actual and possible solutions foreshadowed

Putting the following discussion under the heading of 'solution' is misleading, in that it seems to promise more than could possibly be delivered. There can be no real solid solutions to the transnational Internet within the parameters of national law. Such real solutions lie outside the national-law framework, just as real solutions to the egg industry lay in colour blindness. So it would be more appropriate to refer to these solutions as necessary repair works. Indeed, in some ways, the following summarises the way this book defines the problems and the choices which thereby emerge for regulators. Alternatively, the following discussion picks up on key regulatory themes which run through the competence and the Internet governance debate and invariably through this book.

A. Territoriality: country-of-origin and country-of-destination

Concurrent regulatory claims by States over the same subject-matter often arise because a number of States can in fact make out a territorial link with the activity in question. In other words, the wrongful conduct is 'located' in a number of States. Take, for example, a libellous article in a newspaper published in Norway and Sweden; or the shares of a mismanaged company listed on several stock exchanges; or the Danube polluted in Germany, with the polluted water carried downriver through Austria, Slovakia, Hungary, Croatia, Serbia, Bulgaria, Romania, Moldova and the Ukraine. In all these instances, a number of States or their residents may be affected by the activities and may want to institute civil or criminal proceedings against the wrongdoer. And the same applies to online activity.

In these situations, a dichotomy has developed in the legal debate on competence, particularly in the online context, which distinguishes between the 'country of origin' and the 'country of destination' as alternative or concurrent would-be regulators. In the first instance, the link which may justify regulatory competence is the location of the source of the activity and in the second instance the location(s) of its effects. This dichotomy has traditionally attracted relatively little

attention either in public or in private international law. Nevertheless, in public international law, the distinction drawn between the subjective and objective territoriality principles[68] mirrors the country-of-origin versus the country-of-destination dichotomy. If Bertha in France shoots across the border killing Albert in Switzerland, a murder prosecution against Bertha could be instigated in either country: France, as the country of the crime's 'subject', and Switzerland, as the country of the crime's 'object'. Some private international law principles also reflect or acknowledge the dichotomy. For example, the European Court of Justice has held that a tort may be said to have occurred – for the purposes of determining the competent court – in either the place of the source, or the place of the destination, of the activity.[69]

This country-of-origin and country-of-destination dichotomy has, with some urgency, come to the forefront of the jurisdictional debate on online activity. The problem is not the dichotomy as such, but really any competence rules favouring the country of destination. As is apparent from the above examples, there is generally only one country in which an activity originates, but there may be many in which it has an effect. As most websites by default can be accessed in every country, any country-of-destination or effect-focused rule leads to worldwide competence, and at least theoretically online publishers are expected to comply with the laws of hundreds of States. Thus they have argued for the abolition of destination-centred links. Instead, they argue, only the country of origin of the website should be entitled to regulate it, so online publishers only have to comply with home rules. The argument – while persuasively made by many private actors in different contexts – has, bar a few exceptions, found very little resonance with States. Why States refuse to do so and the price they have invariably to pay for this refusal is explored in Chapter 5.

There is a third way. States have at times, in the private law context, sought to avoid the extreme positions of the outright country-of-origin

[68] Accepted in *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No. 10.

[69] *Shevill and Others* v. *Presse Alliance SA*, Case C-68/93 [1995] ECR I-415, where the European Court of Justice, interpreting Art. 5(3) of the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (1968), held that the harmful event (founding adjudicative jurisdiction in tort cases) occurs either in the place where the damage occurred (country-of-destination) or the place of the event giving rise to it (country-of-origin). See also §145(2)(a) and (b) of the US Restatement (Second) of Conflict of Laws (1971) concerning choice-of-law rules for wrongs.

approach and country-of-destination approach by opting for the middle ground. This middle ground is occupied by a moderate country-of-destination approach, according to which only the States which have been specifically targeted by online activity enjoy regulatory competence. Although this approach avoids some of the theoretical and practical flaws of the extreme positions, it is far from perfect. Ultimately, it is beset by the same enforceability problem as any country-of-destination approach, with the added drawback that some States clearly affected by certain online activity have to abstain from regulation.

B. The Achilles' Heel: limited enforcement jurisdiction

Whatever regulatory claims States may make in principle is one thing, whether they can enforce them is quite another. Enforcement is the focus of Chapter 6. States may legitimately assert the right to make laws for foreign websites and even expose the foreign site operator to court proceedings, but they have no right in any way to enforce these rules or judgments abroad: 'a State . . . may not exercise its power in any form in the territory of another State.'[70] No State can 'send police officers into a foreign State to arrest the criminal and carry him across the frontier, or to send judges into the foreign State to sit there as a court and try the case'.[71] This strictly delimited enforcement power of States is perhaps the single most striking feature of the competence regime in general, and in the online context in particular, and is both a curse and a blessing. Certainly, any arguments for or against a competence rule have a decidedly fanciful and academic air about them if not informed by enforceability, and that applies to any discussion of the country-of-origin versus the country-of-destination.

There is no doubt about it, much of the regulatory conundrum of the Internet is due to States often being unable to give effect to their domestic laws in respect of foreign online activity penetrating their borders – ranging from spam email and misleading advertising, to unauthorised sites offering gambling, pornography and pharmaceuticals. The most straightforward solution would appear to be tinkering with the breadth of enforcement power: if enforcement jurisdiction is too limited, why not expand it? But one State's greater enforcement power is another

[70] *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No. 10, 18. Unless the other State consents.

[71] Mann (1984), above n. 21, 37.

State's loss of territorial control. The strict territoriality of enforcement power protects States from interference by other States within their territory; it protects a State's '[i]ndependence in regard to a portion of the globe [i.e.] ... the right to exercise therein, to the exclusion of any other States, the functions of a State'.[72] In short, it is sacred. The discussion here never asks how enforcement jurisdiction could be altered to accommodate the online world, but rather how States can and do work around it.[73]

Broadly, there are two avenues open to States, apart from simply surrendering regulatory control: do it alone or do it together. This book considers to what extent these avenues have found favour with States, their pros and cons and their future potential. Along the solitary route, States have sought to control foreign websites over which they have no or limited control via those intermediary players on their territory over which they do have control, such as domestic ISPs or financial institutions. But is this always appropriate, feasible or sufficient? Secondly, instead of being lone warriors, States could cooperate. Traditionally, in particular in respect of the criminal law, such cooperation has been extremely limited, which is rather paradoxical as these are the matters of highest priority to States. Nevertheless, '[e]xtreme diffidence is being displayed by States particularly where the execution within their own sphere of sovereignty of foreign criminal judgments or the collection of foreign revenue claims are concerned'.[74] And this is most notable and problematic in relation to those public matters in respect of which States lack harmonised views, such as pornography or gambling. But have States started to soften their harsh stance in view of the rather pressing needs generated by the online world, and, if not, why not?

Last but not least, while it is normal and logical to explore the issue of enforceability after determining the regulatory claims States make in principle, the discussion in Chapter 6 also examines the interrelationship

[72] *Island of Palmas (The Netherlands* v. *United States)* (1928) Reports of International Arbitral Awards 2, 829, 838. Santiago Torres Bernardez, 'Territorial Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 487, 491. Jennings and Watts, above n. 56, 382.

[73] To explore what, if any, inroads have been made into the strict territorial limits of enforcement jurisdiction would seem to be a worthwhile exploration but goes beyond the ambit of this book.

[74] Mann (1984), above n. 21, 37, citing the German Constitutional Court, 22 March 1983, BVerfGE 63, 343, 361.

of these two aspects of jurisdiction. The rather surprising conclusion is that there is clearly a dynamic two-way relationship between regulatory assertions made in principle (legislative and adjudicative jurisdiction) and the power to enforce them (enforcement jurisdiction). Cooperation at the enforcement stage is not just more likely when the regulatory assertion by the other State is moderate, but in fact States moderate their assertions when there is the potential for cooperation. In short, cooperation in enforcement is both a carrot and a stick, and would have a spiralling positive effect on the entire competence framework. This makes it even more pertinent to ask the question why is there not more of it?

C. More global law or a less global internet: a simple choice

Probably the most controversial and uncomfortable idea put forward in this book, in Chapter 7, is that the system of *national* law and the *transnational* Internet are inherently irreconcilable. To resolve that tension, regulators are faced with a very simple choice indeed: either make law more transnational or online activity less transnational. And this is *always* the only choice: there is no middle way, no grey between the black and the white. Just as you cannot squeeze a size 14 person into a size 8 jacket, you cannot hold onto national law whilst at the same time retaining the transnational Internet. That idea may be met with scepticism: how could one make the Internet less global? And does the current legal order not prove that national law and the transnational Internet can co-exist? These questions are addressed in the last chapter, but, briefly at this stage, the general idea is as follows.

Making law more transnational simply entails the harmonisation of substantive legal rules. This can occur either actively (in the form of what is normally understood as international legal harmonisation) or, more often than not, by default. The latter occurs when States are unable or unwilling to regulate a particular online activity *effectively* such as spam or pornography, possibly in favour of self-regulatory mechanisms. Then harmonisation in respect of that activity occurs unwittingly or by default, at the lowest common denominator. For example, if Barbados had no restrictions against pornography, all other States would have to accept the legal standards of Barbados if they are unable to deal with Barbadian pornographic sites. Positive legal harmonisation tends to be presented as the ideal solution to the online conundrum, which it is in the sense that it allows the Internet to be retained as an open medium.

Yet, it does occur at the expense of peculiar national values which, of course, are the very reason why laws have evolved differently in the first place. Alternatively, the conflict between the transnational Internet and national law can be resolved by making online activity less transnational. Initially, this may appear impossible, but in fact it is already happening in various ways.[75] Some oppressive regimes block foreign sites which in any way challenge the official moral or political standards. In Western democratic society, territorial zoning of online activity tends to come in the form of voluntary zoning by online providers. Out of fear of falling foul of a State's laws, the site provider may not allow access to the site or to the goods or services offered on the site in certain States. Alternatively, some large companies create country-specific sites which implement censorship policies consistent with the State's requirements, such as Google does in Germany, France or China.[76] What all these strategies have in common is that they transfer traditional national boundaries into cyberspace – segregating cyberspace into different national cyberspaces. Such territorial zoning allows national policies reflecting peculiar cultural, social and political values to be preserved, but occurs at the expense of the uninhibited freedom of transnational online communications.

So neither harmonisation nor territorial zoning is without drawbacks, and the future of online regulation is likely to be a mixture of both, as indeed it is currently. In other words, while *effective* national law and uninhibited transnational online activity cannot co-exist in respect of the same regulatory field of a State, they can in respect of different fields: a State may decide to try to clamp down on all domestic and foreign

[75] Lucidly discussed in Dan Jerker B. Svantesson, 'Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet' (2004) 23 *John Marshall Journal of Computer and Information Law* 101. See also Jonathan Zittrain and Benjamin Edelman, 'Documentation of Internet Filtering in Saudi Arabia' (2002) Berkman Center for Internet & Society, http://cyber.law.harvard.edu/filtering/saudiarabia/. An example from case law may be *Toys 'R' Us Inc.* v. *Step Two SA*, 318 F 3d 446 (3rd Cir. 2003), where the Spanish company had taken clear steps to strongly discourage customers from outside Spain.

[76] Susan Kuchinskas, 'Google Axes Hate News' (23 March 2005), Internetnews.com, www.internetnews.com/xSP/article.php/3492361/; in respect of China, see Danny Sullivan, 'Google Now Censoring China' (25 January 2006), SearchEngineWatch, http://blog.searchenginewatch.com/blog/060125-072617/; Jonathan Zittrain and Benjamin Edelman, 'Documentation of Internet Filtering Worldwide', in Organization for Security and Co-operation in Europe (OSCE), *Spreading the Word on the Internet* (2003), www.osce.org/item/13574.html; Joel Reidenberg, 'Technology and Internet Jurisdiction' (2005) 153 *University of Pennsylvania Law Review* 1951.

gambling sites and thus uphold its peculiar national gambling laws, but may opt for a *laissez-faire* approach in respect of the online sale of pharmaceuticals and thus retain open global access to all pharmaceutical sites.

While this general idea is rather simple, the diversity of online regulatory problems, as well as the various State responses to them, often hide this inevitable underlying choice. Also, there is no doubt that this choice requires the making of a value judgment by the regulator and ultimately by us:[77] what is more important, our peculiar state laws (reflecting national moral or political standards) or uninhibited global communication? Finally, after that choice has been made, law may help in its implementation but no legal solution can circumvent the choice and allow us to have our cake and eat it.

D. Code: a separate option?

In as much as this book is about regulatory competence, it is also about Internet governance, and this leads to the topic of code. 'Code' has assumed a central role in the Internet governance debate since its 'inception' in Lawrence Lessig's *Code and Other Laws of Cyberspace* and his earlier paper, 'The Law of the Horse: What Cyberlaw Might Teach'.[78] The core idea in these texts is that regulatory objectives may be achieved in a number of ways and only one of them is legal rules imposing obligations coupled with the threat of sanctions for non-compliance. Alternative routes to suppress undesirable behaviour and encourage desirable

[77] One factor feeding into that deliberation is likely to be the cost of territorial zoning in the circumstances.

[78] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Book, 1999); and Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501. For some precedents for Lessig's idea, see, for example, James Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors' (1997) 66 *University of Cincinnati Law Review* 177, www.law.duke.edu/boylesite/foucault.htm. But Lessig's ideas have certainly captured the imagination of many and triggered a substantial discussion on the topic. For but a few examples, see N. Nguy, 'Using Architectural Constraints and Game Theory to Regulate International Cyberspace Behaviour' (2004) 5 *San Diego International Law Journal* 9431; Christian Ahlert, 'Technology of Control: How Code Controls Communication', in Organization for Security and Co-operation in Europe (OSCE), *Spreading the Word on the Internet* (2003), www.osce.org/item/13574.html; Tim Wu, 'When Code Isn't Law' (2003) 89 *Virginia Law Review* 679; Neal Kumar Katyal, 'Digital Architecture as Crime Control' (2003) 112 *Yale Law Journal* 2261; Marc Rotenberg, 'Fair Information Practices and the Architecture of Privacy' (2001) *Stanford Technology Law Review* 1; L. Jean Camp and Serena Syme, 'Code as Governance, the Governance of Code' (2001) John F. Kennedy School Government Faculty Research Working Paper Series, http://ssrn.com/abstract=297154/.

behaviour may lie, depending on the circumstances, in influencing moral or social rules (norms) or in providing financial incentives or disincentives (market)[79] or in changing the physical environment in appropriate ways. This last regulatory route is what Lessig calls code or architecture: regulation through the existence or creation of physical restraints.

This approach of changing the physical environment so as to facilitate certain behaviour and suppress other behaviour is particularly relevant in a man-made environment, which is relatively easily amenable to change, such as the Internet. By changing the technical aspects of the Internet, its functionality may be changed. Such change may not only be designed to increase the convenience and functionality for us users, but also to implement regulatory objectives.[80] A State may use, for example, code in the form of blocking mechanisms, to prevent access to illegal foreign sites. And this is likely to be more efficient than traditional law, achieving almost universal compliance with only little effort needing to go into monitoring and enforcement procedures. However, code as a regulatory tool has rightly been treated with scepticism by liberals for two reasons.[81] First, code, unlike traditional regulation, does not presuppose or require transparency: it can be effective, whether or not those subject to it (as well as later generations) are aware of it.[82] Secondly, code deprives those subject to the law of personal autonomy of the right to decide whether to comply with the law or not and thus of being morally responsible agents.[83] Once code is implemented, one has no choice whether to act this way or that way. But liberal society on the whole 'allows people to make decisions about their action beforehand (treating knowledge of likely legal consequences as

[79] Discussed also in general writing on regulation: for example, Robert Baldwin, Colin Scott and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: Oxford University Press, 1998), 3f.

[80] A classic example would be software protecting copyrighted material, i.e. digital rights management software.

[81] For a lucid discussion, see Roger Brownsword, 'Code, Control, and Choice: Why East Is East and West Is West' (2005) 25 *Legal Studies* 1.

[82] Lessig (*Code*, 1999), above n. 78, 98: 'The state has no right to hide its agenda. In a constitutional democracy its regulations should be public. And thus, one issue raised by the practice of indirect regulation is the general issue of publicity.' He continues (*ibid*., 99): 'Indirectly . . . the government can achieve regulatory ends, often without suffering the political consequences that the same ends, pursued directly, would yield. We should worry about this. We should worry about a regime that makes invisible regulation easier.'

[83] Brownsword, above n. 81, 17ff.

merely one reason for acting in a particular way, which may be outweighed by other reasons)'.[84] And, 'if techno-regulators know how to stop us from being bad only by, at the same time, stopping us from being good',[85] then perhaps code – despite its vast regulatory potential in cyberspace – comes at a price too high to pay.

The pros and cons of code *per se* concern the discussion in this book only marginally. The central question here is how code relates to the competence debate: is it a governance solution separate and outside any competence model? Yes and no. Yes, in so far as (as the brief discussion above shows) code as a regulatory tool has its own clear potentials and raises its own distinct concerns. Therefore, in whatever context it figures, these special characteristics deserve and mandate attention. On the other hand, code is no more (or less) than an available regulatory tool; it comes in at the implementation stage after a principled decision has been made whether an activity should be regulated or not. Code may or may not be used to give efficacy to that policy decision. Being a regulatory tool, it hovers in the background of the competence debate and is a practical consideration taken into account in deciding whether it is feasible or desirable to hold onto national law in the online context. But, as will be shown in the cooperation context, just because code could be used, does not at all mean that it should or will be used – if such usage would clash with an existing regulatory tradition or culture.

In short, code can be, and is, adopted in a wide variety of regulatory approaches. It can go hand in hand with a total hands-off, self-regulatory approach, but equally code may be the decisive weapon of the most invasive State regulation. Code itself has no loyalties or predispositions.

[84] David Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd edn, Oxford: Oxford University Press, 2002), 771.
[85] Brownsword, above n. 81, 20.

2

Law: too lethargic for the online era?

1. National trademarks versus international domain names

The clash between national law and the transnational online world starts with the most basic aspect of the Internet, namely, its address system, the domain name.[1] Johnson and Post in 'Law and Borders – The Rise of Law in Cyberspace' used the conflict of trademarks with domain names (as well as other marks on websites) as the archetypal example to argue for a paradigm shift away from laws based on geographic boundaries, that is, traditional national laws.[2] Their initial statement of the problem captures its essence perfectly and has been echoed innumerable times.

> Consider the placement of a 'traditional' trademark on the face of a World Wide Web page. This page can be accessed instantly from any location connected to the Net. It is not clear that any given country's trademark authorities possess, or should possess, jurisdiction over such placements ... Large US companies may be upset by the appearance on the Web of names and symbols that overlap with their valid US-registered trademarks. But these names and symbols could also be validly registered by another Party in

[1] The names used to identify websites which are more memorable than the 16-number IP addresses which underlie them, such as aber.ac.uk for the University of Wales, Aberystwyth.

[2] David R. Johnson and David Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367. There is plenty of literature on the topic. For more recent discussion, see Richard L. Garnett, 'Trademarks and the Internet: Resolution of International IP Disputes by Unilateral Application of US Law' (2005) 30 *Brooklyn Journal of International Law* 925; Graeme Dinwoodie, 'Trademarks and Territory: Detaching Trademark from the Nation-State' (2004) 41 *Houston Law Review* 885; American Bar Association (ABA), 'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf, esp. 120ff. For discussion of competence in respect of intellectual property rights, see James J. Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (Oxford: Oxford University Press, 1998).

> Mexico whose 'infringing' marks are now, suddenly, accessible from within the United States.[3]

Since then, a decade has passed, confirming the accuracy of this description again and again. Not only has intentional trademark abuse flourished on the Internet,[4] but there have been countless disputes with one legitimate trademark owner, inadvertently through his online activities, encroaching onto the territorial sphere of another equally legitimate trademark owner.[5] These disputes are not easily resolved, especially between two innocent parties each holding legal entitlements to the name within their respective territorial spheres. Indeed, initially it appears that few, if any, online activities – within which the domain name system is an integral and now quite indispensable part – may be carried on without inevitably infringing foreign trademarks; and this seems to lead to the conclusion that either online activity or national trademark law can survive, but certainly not both.

In the early Internet days, many, including Johnson and Post, came precisely to that conclusion. They believed that tinkering with law here and there would simply not be good enough; drastic legal change was needed: 'In this age of cyberspace and global connectivity, reliance on statutes and *stare decisis* simply cannot keep up with a rapidly evolving technological environment. Traditional law [such as *lex mercatoria*], then, might condemn rules regulating conduct in cyberspace to perpetual obsolescence.'[6]

[3] Johnson and Post, above n. 2, 1377.

[4] Generally in the form of cybersquatting, discussed in depth in Graham J. H. Smith (ed.), *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002), Ch. 3.

[5] For a classic early example, see *Prince plc* v. *Prince Sports Group Inc.* [1998] FSR 21, where the English computer company's rights in the unregistered mark clashed with the trademark rights of a US sports equipment company of the same name and both claimed entitlement to prince.com. More recently, in *Toys 'R' Us Inc.* v. *Step Two*, 318 F 3d 446 (3rd Cir. 2003), both US and Spanish toy companies used the name 'Imaginarium' in connection with their products and websites, and the Spanish company was alleged to have infringed the US company's trademark through its website.

[6] Matthew R. Burnstein, 'Conflicts on the Net: Choice of Law in Transactional Cyberspace' (1996) 29 *Vanderbilt Journal of Transnational Law* 75, 110. See also Joel R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 *Emory Law Journal* 911; Robert Reilly, 'Mapping Legal Metaphors in Cyberspace: Evolving the Underlying Paradigm' (1998) 16 *Journal of Computer and Information Law* 579; Aron Mefford, 'Lex Informatica: Foundations of Law on the Internet' (1997) 5(1) *Indiana Journal of Global Legal Studies* 211; Franz C. Mayer, 'Recht und Cyberspace' (1997) 3 *Humboldt Forum Recht*, www.humboldt-forum-recht.de/3-1997/Text.html. For a more conservative later account of the necessary legal changes in response to the online revolution, see Bradford L. Smith, 'The Third Industrial Revolution: Law and Policy for the Internet' (2000) 282 *Recueil des Cours* 229.

The calls for a legal revolution have echoed across many areas of law, and were often based on the territorial ambit of the traditional rules in a non-territorial world, that is, the territorial allocation of regulation competence. Even sober commentators concluded that, for example, the 'trademark system may be in the process of breaking down because markets, many of which historically were relatively local . . . are global on the Internet; there is no such thing as an Internet domain name that is in use only in a geographic area.'[7] Yet the judiciary has rarely, if ever, accepted that the border-defying Internet is beyond national law and the question addressed here is, why? Why are these arguments for the drastic rejuvenation of law in the Internet age – which are so often in themselves compelling – not accepted or acceptable?

The answer to that question throws light not just on the competence debate in the Internet era but also, more generally, on governance at times of significant social or economic change. The main point is that law is like Koala, a lethargic animal, moving at a sleepy pace even when the world rushes past, and not without good reason. The early jurisdiction Internet cases especially serve as a good example to show the type of factors and constraints which feed, and must feed, into legal argumentation *per se*. Moving between the starkly varying assertions on the legal-change spectrum, the discussion exposes some of the flawed assumptions made by legal revolutionaries: assumptions about law and legal change which undermine their legal arguments and conclusions. The discussion introduces the core jurisdictional issues explored in more specific contexts later and the type of concerns the judiciary and legislators take into account to resolve them, as well as the more general parameters for legal argumentation, especially vital in the Internet context which often turns otherwise placid lawyers into raging rebels. First, though, it is useful to categorise more broadly the regulatory problems caused by the Internet and position the jurisdiction problems within them.

2. The Internet's impact on law and regulation

A. The qualitatively new legal problems

The Internet has affected law and regulation in two, often overlapping, ways. First, the technical design of the Internet has allowed for genuinely new ways of interaction and new activities (which is not to deny the existence of some remotely analogous activities in the offline

[7] ABA, above n. 2, 120.

world[8]). These have given rise to myriad genuinely new legal issues. For example, the process of linking on the Internet is novel, and one legal issue which it has raised is whether a link from one website to an inner webpage of another website constitutes copyright infringement.[9] Another new legal problem arises from the ability to sign up to software packages with ongoing updates: for taxation purposes are these packages goods or services?[10] The use of domain names has raised the question whether they should be treated like trademarks and, if so, how the different allocation bases can be made compatible.[11] And this partly overlaps with the central new competence issue: does the mere accessibility of a foreign website provide sufficient justification to make the site and its operator subject to the State's substantive and procedural laws or processes?

These legal questions reflect a common aspect of regulation which is often hidden: 'Legal rules and principles commonly contain not only normative determinations about what ought or ought not to happen under certain circumstances, but also background factual assumptions about the nature of the world.'[12] For example, the factual assumption upon which the rules allocating regulatory competence have relied was that the commercial 'entry' onto a foreign market was almost always the result of deliberate efforts by the business.[13] And such efforts also

[8] For a discussion of the dangers of transplanting legal concepts from the physical world into cyberspace, see Shyamkrishna Balganesh, 'Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass' (2006) 12 *Michigan Telecommunications and Technology Law Review* 265.

[9] For a discussion of the legal issues arising out of web links, see Smith, above n. 3, 32ff. See e.g. the Scottish case of *The Shetland Times Ltd* v. *Wills* [1997] FSR 604 and the US case of *Ticketmaster Corp*. v. *Tickets.com Inc*., WL 525390 (CD Cal. 2000).

[10] See e.g. European Commission, *Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee: Electronic Commerce and Indirect Taxation*, COM(1998) 374 final. Another issue was whether payment for downloaded goods should be classified as trading income or royalty income.

[11] Discussed in depth in Smith, above n. 4, Ch. 3. As technology is developing, other trademark issues arise. See e.g. Nigel Miller, 'Has Your Trademark Been Googled?' (2004) 15 *Computer and Law* 36. Another issue is whether traditional causes of action such as conversion may be applied to intangible chattels, such as domain names: *Hoath* v. *Connect Internet Services* [2006] NSWSC 158.

[12] Frederick Schauer, 'Free Speech and the Demise of the Soapbox' (1984) 84 *Columbia Law Review* 558, 558.

[13] Sometimes, even in the non-Internet context, goods may 'travel' into a foreign State in circumstances where it is beyond the control or knowledge of the business which produced or distributed them. See *World-Wide Volkswagen Corp*. v. *Woodson*, 444 US 286 (1980), where the court concluded that such 'entry' would expose the defendant to the personal jurisdiction of the forum court only if the defendant knew its goods would enter the State in the particular instance or on a regular basis.

tended to be accompanied by some physical entry into the State, either in the form of business premises or, at the very least, with physical goods crossing borders.[14] Similarly, trademark law has relied upon the assumption that businesses tended to operate within a territorially delimited space. These background assumptions have been displaced both by digital technology and the Internet. Even the smallest business, once online, has a global ambit, and special efforts are needed to limit rather than expand its reach. Entering a State in the Internet context is often limited to the entry of digital signals which are – for regulatory purposes – rather elusive. How should the law treat such 'accidental' digital entry into a foreign market?

B. The quantitatively new legal problems

The importance of the background factual assumptions upon which legal rules are based is also illustrated by this type of Internet-related legal problems. These problems arise out of online activity which is not really novel at all. The Internet often allows people to do exactly what they have done before, yet with much greater efficiency. Such activities do not raise any genuinely new legal issues in the strict sense and at first 'seem wholly unremarkable'.[15] Yet, their ordinariness is deceptive, as they question the efficacy of legal regimes which had previously relied upon the impracticability of engaging in certain conduct. The Internet has again had the effect of rebutting the factual assumptions underlying certain legal regimes. For example, in relation to defamation, it has been said that:

> there is nothing very new . . . [about online defamation], which is, formally, true – but the problems of traditional publishing and defamation are so multiplied when applied to a forum as large, as accessible, as cheap and as transnational as the Internet, that is not hard to see why there is a perception that the law of libel has been transformed by its application to the new electronic highway.[16]

[14] Although not always, e.g. television signals: *Groppera Radio AG* v. *Switzerland* (1990) 12 EHRR 321, where the applicant had broadcast from Italian territory radio programmes intended for the Swiss and redistributed on Swiss territory by Swiss cable companies. Swiss regulation of these cable transmissions was upheld.

[15] I. Trotter Hardy, 'The Proper Legal Regime for "Cyberspace"' (1994) 55 *University of Pittsburgh Law Review* 995, 999.

[16] Lilian Edwards, 'Defamation and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet – Regulating Cyberspace* (Oxford: Hart Publishing, 1997), 183, 184.

The law of copyright has to some extent relied upon the factual assumptions that reproduction will lead to a loss of quality and that the marginal costs of reproduction and distribution will outweigh the benefits achieved by infringement.[17] However, in the digital age, an unlimited number of perfect copies can be made and distributed at minimal cost. Also, in the taxation context, 'the Internet currently does not present new or difficult problems for transfer pricing ... However, the growth of the Internet is making some of the more difficult transfer pricing problems more common ... The speed, frequency, anonymity and integration of exchanges over the Internet will place great pressure on the transactional methodologies and comparability principles'.[18]

This sort of quantitative problem also affects regulatory competence. Callinan J describes the 'unremarkable' jurisdictional change:

> In the past 'The Times' newspaper would have gone to every colony in Australia. It might have got there rather late, but it would have gone to every colony in Australia, every province in Canada, it would have gone throughout the whole of that part of the world which was coloured red. I do not see the Internet as introducing anything particularly novel, you just get it more quickly.[19]

But, perhaps, 'just getting it more quickly' is not quite as unproblematic as it seems. The relatively complex jurisdictional regimes under private and public international law have implicitly placed reliance on the fact that physical distance provides a disincentive for the average consumer and business to engage in international transactions and that therefore, for example, most retail transactions are localised within a State. If the Internet turns transnational conduct and transactions from being the exception to being the norm – because it is as easy and cheap to interact with a geographically remote area than with one that is physically close – current jurisdictional regimes may prove unworkable. This is not because the relevant legal regimes do not provide the answers to

[17] Eric Schlachter, 'The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet' (1997) 12 *Berkeley Technology Law Journal* 15, 19f. Smith, above n. 4, 14f, 50, where the writer also expresses the common speculation whether copyright law may soon be replaced by contractual arrangements.

[18] Australian Taxation Office, *Tax and the Internet*, Discussion Report of the ATO Electronic Commerce Project (1997), 63.

[19] Transcript of Proceedings, *Dow Jones & Co. Inc.* v. *Gutnick* (28 May 2002, High Court of Australia), www.austlii.edu.au.

particular disputes but because it would simply be impracticable to use them.[20] For example, in principle there may be no doubt whatsoever about the legal rights in a particular transnational online retail transaction, but the practical difficulties and costs of using a foreign court, a foreign language and a foreign legal system to enforce them are likely to far outweigh any benefits of doing so.

C. The severity of the problems

Many areas of law have been affected by both the qualitative and the quantitative problems. As a matter of general assessment two points need to be made. First, the qualitative problems have had an immediate bearing upon the law; they have given rise to novel disputes and conflicts which required relatively immediate adjustments of the law, with some legal change or addition being inevitable. On the other hand, the quantitative problems have a more distant and diffuse impact upon the law in the sense that they do not lead to disputes which are in any obvious way novel. Paradoxically, while their long-term impact on the law is potentially more fundamental because they attack the very roots of certain legal regimes, ostensibly no legal change is required. At least the judiciary would be hard pressed to find any valid reason for distinguishing such online cases from existing offline cases. A classic statement which reflects this is that of Callinan J in *Dow Jones & Co. Inc.* v. *Gutnick*, responding to arguments about the ubiquity of the Internet: 'Some brands of motor cars are ubiquitous but their manufacturers, if they wish to sell them in different jurisdictions, must comply with the laws and standards of those jurisdictions. There is nothing unique about multinational business.'[21] He sees no difference between traditional multinational businesses and online businesses because *in principle* there is none. But this merely disguises the fact that there is a vast quantitative difference between these businesses: the former, unlike the latter, have tended to be huge businesses and thus capable of absorbing the cost of having to comply with the laws of a number of States. Many online businesses, on the other hand, are small and cannot realistically be expected to comply with more than one set of laws. So, although the judiciary may

[20] The efficiency of the current nation-state legal allocation model is dependent upon the general location of legally relevant events within nation states.

[21] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 186.

not find any valid point of distinction, there can be no doubt that the quantitative problems are far from harmless.[22]

Secondly, it seems fair to assert that the jurisdictional problems, both qualitative and quantitative, deserve special attention. Their impact is not limited to any particular area of law: they affect the very foundation upon which these areas of substantive regulation are based. Not surprisingly, the jurisdictional challenges in the Internet era led to extreme viewpoints on the extent of the legal change required. These were reflected in the differing legal metaphors and analogies suggested, especially in the early days, to illuminate the problems and appropriate solutions. Some held that the Internet is just another communication tool, with analogies to physical publication and distribution channels or existing communication facilities being appropriate. They yielded to the natural 'temptation to analogize new electronic media to existing technology for which ... [one] already [has] models to rely upon'.[23] Others disagreed.[24] They said that the Internet requires a whole new approach. In a search for the right analogies, these writers went generally much further back in legal history. For the governance of the Internet they proposed models such as *lex mercatoria*, admiralty law, or the law applying to common resources such as Antarctica, outer space or the high seas.[25] They asserted that the Internet is more than a quantitative step in the evolution of information technology and thus requires more than a mere adjustment of the law. A failure to appreciate, they said, is to repeat the mistake made in the past by, for example, those who assumed that printing was just a technological replacement of writing and thus failed to realise that printing was qualitatively different from writing and raised fundamentally new legal issues.[26] How are these very different conclusions arrived at?

[22] Trotter Hardy, above n. 15, 1000.

[23] Reilly, above n. 6, 583. Typically done by the judiciary: see, for example, *Maritz Inc.* v. *Cybergold Inc.*, 947 F Supp 1328 (ED Mo. 1996), where the court used the analogy to postal mail to decide that the defendant was transmitting its advertising into Missouri and thus was subject to the jurisdiction of the Missouri court.

[24] See, e.g., Johnson and Post, above n. 2, 1374, in which the authors criticise those who treat 'the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographic location to another'. See also Dan L. Burk, 'Jurisdiction in a World Without Borders' (1997) 1 *Virginia Journal of Law and Technology* 1522.

[25] For some examples of those early academic views, see above n. 6.

[26] Reilly, above n. 6, 581.

3. Legal reasoning and legal change

A. Legal reasoning

Generally, legal argumentation or reasoning is a non-issue. When legal issues call for solutions, the proper method of legal argumentation is not raised to a conscious level. This is so even though it is clear that the right approach to legal argumentation, whether by academics, legislators or the judiciary, is critical for arriving at valid conclusions: 'some methods . . . work better than others. Some yield conclusions that do not stand the test of further situations; they produce conflicts and confusion; decisions dependent upon them have to be retracted or revised.'[27] Generally, it is simply assumed that legal issues are determined 'by the staple processes of legal reasoning, namely, induction and deduction from earlier decisions and settled rules and practices'.[28] Sometimes though – some contend – these staple processes are inadequate:[29] 'reliance on statutes and *stare decisis* simply cannot keep up with a rapidly evolving technological environment.'[30] But what are the alternatives? Is the concept of *stare decisis* in its widest sense not a critical aspect of the rule of law which cannot be abandoned even in the face of the most challenging new social and economic phenomena? Is a clean slate approach ever an option?

First of all, legal reasoning – the process of argumentation or 'the act . . . of forming reasons, drawing conclusions, and applying them to a situation under consideration'[31] – is employed by all those who need to justify their decisions or actions against some legal standards.[32] At the national

[27] John Dewey, 'Logical Method and Law' (1924) 10 *Cornell Law Quarterly* 17, 19.

[28] *Dietrich* v. *The Queen* (1992) 177 CLR 292, para. 4 (Deane J).

[29] *Ibid*,: there may be rare cases 'in which those processes . . . are inadequate in a developing area of the law or in which a court . . . concludes that the circumstances are such that it is entitled and obliged to reassess some rule or practice in the context of the current social conditions, standards and demands and to change . . . the direction of the development of the law'. In *Jaensch* v. *Coffey* (1984) 155 CLR 549, 600, Deane J seems to resile partly from his initial comment that adherence to precedents may in rare cases not be appropriate, when he said that '[e]ven in such a case, however, the distinction between judicial and legislative functions should never be forgotten and any reassessment of the content of relevant rules should be approached with due regard to *existing authority and established principle*' (emphasis added).

[30] Burnstein, above n. 6, 110.

[31] Kent Sinclair, 'Legal Reasoning: In Search of an Adequate Theory of Argument' (1971) 59 *California Law Review* 821, 824.

[32] Neil MacCormick, 'The Artificial Reason and Judgement of Law', in Aulis Aarnio and Neil MacCormick (eds.), *Legal Reasoning* (New York: New York University Press, 1992), Vol. 1, 167, 167.

level those standards may be fairly readily ascertainable from statutes, regulations or decided cases. In contrast, it has been argued that the absence of clearly defined international standards means that:

> [*I*]*nternational law* . . . does not easily lend itself to brilliant argument by counsel. Instead it has to be assessed as a common pattern of state practice with great care and considerable pedantry. International lawyers have to engage in a time consuming search for bits of state practice, to collect them under some systematic headings and then to draw very modest conclusions as to their common denominator based on *opinio juris*.[33]

While there is no doubt some truth in this argument, it ignores the existence of fairly clear and precise statements of international law in treaties, and it also wrongly implies that the difficulty of ascertaining a particular legal standard adversely affects the process of argumentation after that standard has been ascertained. International law may not lend itself to brilliant argument by counsel, but of necessity and as a matter of practical experience it lends itself to legal argumentation.

Related to the question of who engages in legal reasoning, is the issue as to the extent to which any discussion on legal reasoning must be forum-specific – not unimportant for this book which jumps across legal systems. Most analyses of legal reasoning are forum-specific,[34] and indeed focus on the process of argumentation in one particular segment of domestic law.[35] Nevertheless, '[t]hat there are . . . differences of national style, tradition and canons of argumentative elegance need not be disputed, . . . [but s]o far as legal systems include rules which it is mandatory to apply in every case to which they clearly refer, observance of the requirements of deductive logic is a necessary element in legal justification. That is an analytic truth'.[36] Thus, at the risk of

[33] Karl M. Meessen, 'International Law Limitations on State Jurisdiction', in Cecil J. Olmstead (ed.), *Extra-Territorial Application of Laws and Responses Thereto* (Oxford: International Law Association and ESC Publishing Ltd, 1984), 39.

[34] Some commentators have expressly stated that their analyses of legal reasoning apply to all legal arguments or have a wider bearing beyond the particular context selected. See, for example, Sinclair, above n. 31, 834f; Robert S. Summers, 'Two Types of Substantive Reasons: The Core of a Theory of Common-Law Jurisdictions' (1978) 63 *Cornell Law Review* 707, 709f. Note also Dewey, above n. 27, 24, who comments on the common origins of legal argumentation.

[35] Such as judicial reasoning at first or at the appellate level. For an example, see Summers, above n. 34. For an analysis of lawyer's reasoning, see Julius Stone, *The Legal System and Lawyers' Reasoning* (Stanford: Stanford University Press, 1964).

[36] MacCormick, above n. 32, 170.

sounding banal, it is universally true that a rule – whether extracted from statute or case law – applicable to certain situations must be applied when a situation of that type arises. Admittedly, differences exist in the process of establishing the applicable rules: common law relies on the judge's ability to extract mandatory rules from cases and tends to favour a more pragmatic disposition 'proceeding more cautiously case by case, never generalising a principle further than present need, always distrusting the pursuit of any principle to its ostensibly "logical" conclusions'.[37] This, coupled with the power of common law judges to overrule a pre-established rule in certain circumstances,[38] caters for greater judicial activism in common law jurisdictions.[39] It may also translate into a greater acceptability of bolder arguments in common law courts than in courts of jurisdictions relying on codified law (perhaps explaining the need for greater legislative activism in civil law jurisdictions in response to the Internet).

B. Judicial reasoning: continuity and change

How does the law change and respond to social and economic change? To what extent is and should legal reasoning be responsive to non-legal considerations? The assertion that all legal reasoning is deductive in nature presupposes the existence of a mandatory rule clearly applicable to certain facts. However, it provides little guidance on how cases are or should be argued, decided and justified where there is no clearly applicable rule or where there are conflicting rules, and on how choices between them are or should be made.[40] This problem applies especially to cases arising out of radically new phenomena, such as the Internet, because existing rules were not at all designed with the particular phenomenon in mind. What considerations are or should be taken

[37] MacCormick, above n. 32, 171.

[38] The House of Lords, for example, can overrule its own decisions since the Practice Statement of 1966 which allows it to adapt the law to changing social conditions.

[39] Judicial activism is of course not unknown in civil law jurisdictions. For example, the German Constitutional Court (*Bundesverfassungsgericht*) has been extremely active and influential since its inception in 1951. Friedrich Karl Fromme and Hermann Dornhege, '"Die Entscheiding is unanfechtbar" Das Bundesverfassungsgericht', No. 6 (1997) *Deutschland – Zeitschrift für Politik, Kultur, Wirtschaft und Wissenschaft* 24.

[40] Contra Sinclair, above n. 31, 839, who argues against the proposition that in penumbral cases deduction has 'at the most a trivial role to play; only after the real issue in the analysis has been decided . . . is a conclusion . . . deducible'.

into account when such very novel cases call for decisions? It has been suggested that:

> Especially in times of dynamic social or economic change, a style of judging which confines itself to deductive/subsumptive reasoning from pre-established rules or precedents may appear unattractive compared with more forward looking, goal-oriented types of reasoning. What makes a decision right is not how it matches up to some postulated norm of rightness, but its potentiality to contribute to some improvement in the state of affairs now or in the future.[41]

Such a forward-looking approach is attractive in that it is explicitly intended to facilitate change.[42] Yet it is fraught with danger, partly because it relies on an ability to accurately predict the future. More importantly, adopting an unqualified 'logic of prediction of probabilities rather than one of deduction of certainties'[43] does not sit easily with the need to maintain continuity of the law. If law was ever-changing in immediate response to an ever-changing society, there would be no law; a rule in constant flux is no rule at all.[44] The 'rule of law' implies some adherence to legal tradition and to the concept of *stare decisis*, to fulfil its basic function to 'answer to the need for certainty, predictability, order and safety'.[45] This often mistakenly gives rise to the complaint that '[o]nly *the Law* resists and resents the notion that it should ever change its anticipated ways to meet the challenge of a changing world'.[46] In fact, resistance to change is an essential element of law.

[41] MacCormick, above n. 32, xii, commenting on Dewey's analysis in the same book.

[42] This approach has sometimes been termed the pragmatic approach, as opposed to the principled approach to argumentation: see e.g. P. S. Atiyah, 'From Principles to Pragmatism: Changes in the Function of the Judicial Process and the Law' (1980) 65 *Iowa Law Review* 1249. For a criticism of either approach, see Neil MacCormick, 'On Legal Decisions and Their Consequences: From Dewey to Dworkin' (1983) 58 *New York University Law Review* 239, 239f.

[43] Dewey, above n. 27, 26 (emphasis added).

[44] In the context of international law, see Michael Byers, *Custom, Power and the Power of Rules* (Cambridge: Cambridge University Press, 1999), 49: 'there would be no point in having rules of international law if those rules were, at least, potentially in a continuous state of flux. Indeed, the essence of obligation and the purpose of law would seem to be an ability to control both present *and* future behaviour.' And, at 19: 'although these shared understandings apply generally to all State behaviour, they are not static, but instead undergo subtle modifications as the international system evolves.'

[45] Vilhelm Aubert, *Continuity and Development in Law and Society* (Oslo: Norwegian University Press, 1989), 76.

[46] Fred Rodell, *Woe Unto You, Lawyers*!, cited in Reilly, above n. 6, 589.

Yet, stability and certainty cannot be achieved by attempting to squeeze a new phenomenon into an old jacket: 'to claim that old forms are ready at hand that cover every case . . . is to pretend to a certainty and regularity that cannot exist in fact. The effect of that pretension is to increase practical uncertainty and social instability.'[47] Nevertheless, the conscious regard to the past is crucial to ensure a smooth and predictable transition from the old to the new. The apparent conflict between the need to acknowledge pre-established rules and the need to facilitate change in view of changing social and economic conditions is largely illusory in so far as it affects legal reasoning. Any ruling concerning a new phenomenon – which every new case *is* to a greater or lesser extent – is justified by both forward-looking '*consequentialist* arguments showing the acceptability or unacceptability of . . . [it] one way or the other having regard to their consequences and by [backward-looking] arguments of *coherence* and *consistency* showing how . . . [it] can fit within the existing relevant body of law, i.e., can fit with the legal system as already authoritatively established'.[48] This explains how law can be both static and dynamic, how it changes, yet at the same time continues on its trodden path. It also shows that successful legal reasoning must be governed by an appreciation of the essentially incremental development of law; incremental in the sense that past rules are always a necessary but not exclusive consideration in arriving at a new ruling.

C. Legislative justification: change and continuity

It may be objected that legal reasoning must be informed by pre-existing rules only in the judicial context. Legal arguments for the need for new legislation or treaties need not be restricted by existing anachronistic rules, that is, the very rules the abolition of which is advocated. Suffice to say that, although the legislature is not generally bound by pre-established rules,[49] and is, and indeed must be, strongly present and future oriented, it still owes and pays respect to the past. Legislative reforms take as their starting point existing statutes or rules generally, which in turn were the outcome of previous reforms. Furthermore, these reforms must fit, in terms of coherence and consistency, within the

[47] Dewey, above n. 27, 26

[48] MacCormick, above n. 32, 175. Byers, above n. 44, 9: 'Legitimacy in international law is derived at least partly from internal coherence'.

[49] Obvious exceptions are rules contained in constitutions, and international law.

established legal system, similar to judicial pronouncements.[50] And, although the legislature's power to make sweeping legal changes (which also build on the foundation of the existing law) is greater than that of the judiciary, it has to be exercised rarely and with self-restraint if certainty and predictability, and ultimately social and economic stability, are to be retained: 'Too much change in the law does not simply result in bad law; it results in something that is not properly called a legal system at all.'[51] While principles of legal reasoning – the process of justification of conduct or decisions against pre-existing legal standards – do not strictly apply to arguments for legislative reform, they still must be guided by an appreciation of the law's inherent orientation to the past.

For the purpose of this discussion, the difference in terms of legal reasoning between the legislature and those actors who are expressly bound by pre-established legal standards may be viewed as no more than a matter of degree;[52] with the legislature being able, and under a duty, to emphasise that side of the coin which looks to present and future social and economic conditions. However, 'it will be found that many of the sorts of reasons given for legislative decisions by legislators are not essentially different from those given by judges. Fairness, justice, the rights of individuals, the public interest, all these enter significantly into political as well as judicial law-making'.[53] In short, legal reasoning must always be guided by a recognition of any legal regime's inherent resistance to change, in particular major change, and of the essentially incremental nature of legal change, with new layers of law imposed over the old. What follows is a discussion of the methods of argumentation employed to resolve the new Internet-related jurisdictional disputes, in light of the above general comments.

[50] Even though the legislature can make the old fit the new, often the clear aim of legislative reform is to make the new fit the old.

[51] Lon L. Fuller, *The Morality of Law* (New Haven: Yale University Press, 1964), 39.

[52] Differences between legislative and judicial law-making are, first, judicial law-making 'is subordinate law-making. Parliament can override judicial decisions, while judges cannot override what Parliament does . . . Secondly, Parliament can legislate on its own initiative, while the court can only make law when an appropriate case is brought before it . . . Thirdly, Parliament's law-making powers are vastly more extensive than those of the courts.' P. S. Atiyah, *Law and Modern Society* (Oxford: Oxford University Press, 1983), 131.

[53] *Ibid*., 134.

4. The jurisdictional challenge

A. Is a website enough? Two schools of thought

Is the accessibility of a foreign website a sufficient nexus for an assertion of regulatory competence over the foreign entity or person behind the site? This question has from very early on attracted attention in the various legal contexts and resurfaces throughout this book. The discussion below focuses not so much on the substantive arguments in favour of one position or another but rather on the general paths the arguments follow, comparing the way some academics have approached the issue with the way most judges have dealt with it.

A typical early academic school of thought, with Johnson and Post being prime examples,[54] argued that the Internet showed no regard for territorial boundaries and that the logical consequences of applying national law to foreign websites electronically 'present' within a State were untenable:

> assertions of law-making authorities over Net activities on the ground that those activities constitute 'entry into' the physical jurisdiction can just as easily be made by any territorially-based authority. If Minnesota law applies to gambling operations conducted on the World Wide Web because such operations foreseeably affect Minnesota residents, so, too, must the law of any physical jurisdiction from which those operations can be accessed.[55]

This then means that 'no physical jurisdiction [i.e. no State] has a more compelling claim than any other to subject these events exclusively to its laws'. From there, it seems but a small leap to conclude that, because every State would have a right to regulate every site, no State has such a right. National law is simply unworkable in cyberspace and must be abandoned in favour of cyberspace's own distinct law.[56] This argument – based on the logical consequences of applying existing territorially based rules to websites which are accessible everywhere – is so compelling that it is hard to see how anyone could refuse to follow it.[57]

[54] Johnson and Post, above n. 2. For other academic discussion along similar lines, see above n. 6.

[55] Johnson and Post, above n. 2, 1374. [56] *Ibid*., 1379.

[57] Having said that, the conclusion lacks practical merit in that it fails to answer questions like: how can parties to online transactions order their affairs according to new norms and doctrines which still need developing? Where and how will these norms be enforced? How long shall governments wait for the rise of responsible law-making institutions within cyberspace? What should domestic courts do in the meantime when confronted with Internet disputes?

Yet, judges have done precisely that – even though they routinely accepted the initial premise that online presence alone would give every State regulatory competence and that this is not condonable. For example, in one of the earliest cases on competence, *Playboy Enterprises Inc*. v. *Chuckleberry Publishing Inc*., the judge wisely acknowledged that the defendant 'cannot be prohibited from operating its Internet site merely because the site is accessible from within one country in which its product is banned. To hold otherwise would be tantamount to a declaration that this Court, and every other court throughout the world, may assert jurisdiction over all information providers on the global World Wide Web . . . [which] would have a devastating impact on those who use this global service.'[58] But, despite generally accepting that the accessibility of a website cannot justify an assertion of jurisdiction over the entity behind the site, they have never rejected geographically based laws or processes. In *People of Vacco* v. *Lipsitz*, the court expressly noted that, 'although Internet transactions might appear to pose novel jurisdictional issues, traditional jurisdictional standards have proved to be sufficient to resolve all civil Internet jurisdictional issues raised to date, refuting the view of [those who] . . . believe a new body of jurisprudence is needed'.[59] How have courts been able to justify their assertions despite their support for the argument that an assertion of jurisdiction based on the accessibility of a website is not rationally defensible?

The answer is simple: they have had the benefit of making their principled decisions in the finely textured context of actual cases. This factual context has allowed them to draw distinctions between different cases involving online conduct. Sites differ. The richest body of jurisprudence which clearly illustrates the contextual nature of the decisions is the US case law on adjudicative jurisdiction, mainly in civil matters, and often in trademark cases.[60] In these cases, courts have drawn distinctions between sites that are intentionally targeted at the State or

[58] 939 F Supp 1032, 1039 (SDNY 1996); see also *Digital Equipment Corp*. v. *Altavista Technology Inc*., 960 F Supp 456, 462f (D Mass. 1997).

[59] 663 NY S 2d 468, 473 (NY Sup. 1997).

[60] The seminal US authority in respect of adjudicative jurisdiction in civil Internet cases generally is the trademark case of *Zippo Manufacturing Co*. v. *Zippo Dot Com Inc*., 952 F Supp 1119 (WD Pa 1997). For an early decision made outside the US, see the English decision in *Mecklermedia Corp*. v. *DC Congress GmbH* [1998] 1 All ER 148.

In Internet trademark cases, private international law issues tend to be restricted to the question of adjudicative jurisdiction rather than applicable law; noted e.g. by Garnett, above n. 2, 932. The reason appears to be that, to establish the adjudicative jurisdiction of the court, reliance is invariably placed on the notion of 'specific personal

could be presumed to be so targeted and sites that are not so targeted, distinctions between passive and interactive websites, between commercial and non-commercial websites,[61] between parties who had other offline contacts with the State and those who had not,[62] and between websites that happen to have an effect in the State and sites which were directed at, and known to cause harm in, the State.[63] While initially at least some of these distinctions were hotly disputed, a few years and some fine-tuning later they have developed into fairly settled law. They certainly were comfortably applied in the 2003 case of *Toys 'R' Us Inc.* v. *Step Two SA*, [64] where the interactive nature of the commercial website of a Spanish company was held to be by itself, and in the absence of actual interactions with forum residents,[65] insufficient to expose the company to the adjudicative jurisdiction of the New Jersey court.

jurisdiction' which under its second prong requires that 'the plaintiff's claim arises out of the defendant's activities which were directed at the State'. So to establish adjudicative jurisdiction it is necessary to show that the wrongful conduct was directed at the forum, i.e. the wrongful conduct place, or had its effect, in the forum. This necessarily pre-empts any applicable law inquiry, according to which the law of the place where the wrongful conduct occurred (*lex loci delicti*) governs the trademark dispute. ABA, above n. 2, 122. See also *Ibid*., 123: trademarks like 'all intellectual property benefits from the conventional idea that intellectual property is a form of property and only the forum where the property is located . . . [e.g. by virtue of its registration] has jurisdiction to adjudicate and legislate with respect to that property.'

[61] These distinctions flow from the sliding-scale test established in *Zippo Manufacturing Co*. v. *Zippo Dot Com Inc*., 952 F Supp 1119 (WD Pa 1997). For further discussion of the test, see Chapter 3. Examples of passive websites: *Bensusan Restaurant Corp*. v. *King*., 937 F Supp 295 (SDNY 1996) and *Cybersell Inc*. v. *Cybersell Inc*., 130 F 3d 414, 418 (9th Cir. 1997). Note that it has been increasingly accepted that the interactive nature of the site *per se*, in the absence of any directing of the site at the forum, is insufficient to found personal jurisdiction: *Millennium Enters Inc*. v. *Millennium Music LP*, 33 F Supp 2d 907 (D Or. 1999) and *ALS Scan Inc*. v. *Digital Service Consultants Inc*., 293 F 3d 707 (4th Cir. 2002). Contrast with, for example, *Inset Systems Inc*. v. *Instruction Set Inc*., 937 F Supp 161 (D Conn. 1996). Non-commercial websites tend to be involved in defamation cases: *Young* v. *New Haven Advocate*, 315 F 3d 256 (4th Cir. 2002).

[62] For example *Heroes Inc*. v. *Heroes Foundation*, 958 F Supp 1 (DDC 1996) and *Euromarket Design Inc*. v. *Crate and Barrel Ltd*, 96 F Supp 2d 824 (ND III. 2000).

[63] A classic example of the effects doctrine in this context is *Panavision Intern LP* v. *Toeppen*, 141 F 3d 1316 (1998).

[64] 318 F 3d 446 (3rd Cir. 2003), followed more recently, for example, in *ITP Solar Technologies Inc*. v. *TAB Consulting Inc*., 413 F Supp 2d 12 (DNH 2006); *Sanitec Industries Inc*. v. *Sanitec Worldwide Ltd*, 376 F Supp 2d 571 (D Del. 2005); and *Dluhos* v. *Strasberg*, WL 1683732 (DNJ 2005).

[65] The two sales to an employee and the attorney of the plaintiff company 'presented only inconclusive circumstantial evidence to suggest that Step Two targeted its web site to New Jersey residents.' *Toys 'R' Us Inc*. v. *Step Two SA*, 318 F 3d 446, 454 (3rd Cir. 2003).

Interestingly, too, outside the US, some courts have come to not dissimilar distinctions and conclusions. For example, in the Scottish trademark case of *Bonnier Media Ltd* v. *Greg Lloyd Smith*,[66] Lord Young, seeking to localise the alleged online wrong, recognised that a website may expose the operator to potentially worldwide liability but avoided that very conclusion by adopting a variation of the 'targeting' approach:

> It is obvious that the overwhelming majority of websites will be of no interest whatsoever in more than a single country or small group of countries. *In my opinion a website should not be regarded as having delictual consequences in any country where it is unlikely to be of significant interest* . . . In determining whether the impact of a website is insignificant, it is appropriate in my opinion to look both *at the content of the website itself* and at the *commercial or other context in which the website operates*.[67]

For present purposes, what is significant is not the validity of the distinctions drawn but rather their origin. They were born out of, and informed by, the backward-looking imperative to reconcile the ruling with existing jurisdictional principles,[68] as well as by the forward-looking imperative to avert the consequences of saying either that the accessibility of every website justifies an assertion of jurisdiction, or indeed the opposite. The consequences of the first option 'would [be to] eviscerate the personal jurisdictional requirement'[69] and also raise 'the

[66] *Bonnier Media Ltd* v. *Greg Lloyd Smith and Kestrel Trading Corporation* (Court of Session, Scotland, 1 July 2002), www.scotcourts.gov.uk/opinionsv/dru2606.html.

[67] *Ibid*., para. 19 (emphasis added). Consistent with the English cases of *800-Flowers Trade Mark* [2000] FSR 697 and *Euromarket Designs Inc*. v. *Peters* [2000] ETMR 1025. Also consistent with the German decision of *Re the MARITIM Trade Mark* [2003] ILPr 17, where the court held that the mere online advertisement of a service provided abroad and primarily directed at a foreign market is not a sufficient use of the mark in the forum to amount to a trademark infringement. But note, in contrast to the US jurisprudence on the matter, that that result was reached at the choice-of-law stage rather than the jurisdictional stage (where the court adopted an extremely wide test to catch foreign online providers).

[68] However, many have criticised the distinctions (proposed in *Zippo Manufacturing Co*. v. *Zippo Dot Com Inc*., 952 F Supp 1119 (WD Pa 1997)) as not backward-looking enough, arguing that Internet contacts should not be treated differently from offline contacts; for example 'No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet' (2003) 116 *Harvard Law Review* 1821 (note); Titi Nguyen, 'A Survey of Personal Jurisdiction Based on Internet Activity: A Return to Tradition' (2004) 19 *Berkeley Technology Law Journal* 519; A. Benjamin Spencer, 'Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network Mediated Contacts' (2006) *University of Illinois Law Review* 71.

[69] *McDonough* v. *Fallon McElligott Inc*., 40 USPQ 2d (BNA) 1826, 1829 (SD Cal. 1996).

possibility of dramatically chilling what may well be "the most participatory marketplace of mass speech that . . . the world . . . has yet seen"'.[70] On the other hand, not asserting jurisdiction over any entity simply because it uses the Internet would allow those entities 'to insulate themselves against jurisdiction in every state, except in the state (if any) where they are physically located'.[71] While both of these options are theoretical possibilities within the existing US jurisdictional regimes, the legal, social and economic implications of either are too far-reaching, too revolutionary, to be acceptable.[72] Effectively, the two extreme options have marked the outer boundaries within which courts have established different groups of website cases. Taking the middle path, courts have taken the view that *some* websites, rather than *no* or *all* websites, justify an assertion of jurisdiction.

To what extent the various distinctions drawn in these cases are indeed valid or viable need not concern us now. More important at this stage is the realisation that the law has evolved despite seemingly compelling arguments that it could not. Actual cases not only provide a tool to achieve this, but also illustrate the potential pitfalls of legal argumentation based on over-simplified, too generalised factual premises. Although Johnson and Post admit that '[c]yberspace is not a homogenous place',[73] they close their eyes to the fact that online conduct comes in all shapes and sizes and is not a uniform phenomenon, even in terms of its alleged territorial insensitivity. In actual fact, online conduct does not inherently defy the process of localising behaviour and events comparable to the localisation of traditional activity. Of course, not all traditional points of differentiation and classification are easily transferable to the online world; some have to be revised or even discarded in favour of new or more subtle ones. But it does not mean that every website is as much here as it is there.

[70] *Digital Equipment Corp* v. *Altavista Technology Inc.*, 960 F Supp 456, 463 (D Mass. 1997). See also ABA, above n. 2, 60, arguing that the mere accessibility of a site cannot provide the touchstone for jurisdiction as it would be detrimental to online conduct as well as undermine 'an evolving and necessary system of internationally accepted jurisdictional principles'. This is not to say that courts have never come extremely close to a holding implicitly endorsing worldwide jurisdiction as, for example, in *Inset Systems Inc.* v. *Instruction Set Inc.*, 937 F Supp 161 (D Conn. 1996) or *Cable News Network LP* v. *CNNews.com*, 177 F Supp 2d 506 (ED Va 2001).

[71] *Digital Equipment Corp.* v. *Altavista Technology Inc.*, 960 F Supp 456, 471 (D Mass. 1997).

[72] Acknowledged, for example, in *Hearst Corp.* v. *Goldberger*, WL 97097 (SDNY 1997), 20.

[73] Johnson and Post, above n. 2, 1379.

Judges have been able to reinvent the law in light of the online scenario because the law has constantly evolved in the past in response to a changing world. While it seems that the Internet is totally new and unprecedented, in many ways it is no more than the epitome of a long-standing development towards greater and greater economic globalisation; and these developments have not gone unnoticed by the law:

> [T]he personal jurisdiction problems posed by virtual commerce and Internet telepresence are in many ways the culmination of a long evolution of legal doctrine occasioned by changing technology. Traditionally, jurisdiction over the person was premised on the physical presence of the individual in the forum ... [I]ncreased physical mobility due to automobiles and other modern transportation placed this jurisdictional basis under severe strain ... As a response to the imminent collapse of jurisdiction based on physical presence, the Supreme Court configured new rules upon a kind of 'virtual' presence.[74]

So the continuous evolution of legal rules parallel to the evolution of the media contributes towards reducing the need for drastic legal changes in response to an apparently revolutionary technological development, such as the Internet.

B. Conservatism: a mere result of the judiciary's limitations?

That the law can evolve gradually is one thing, but whether it should is another. It may be argued that the courts' moderate and incremental approach in these cases is typical for judicial reasoning and reflects the restraints to which courts are subject. Therefore, it may be argued, the above cases do not provide insights for the process of argumentation generally or comment in any way on the need for, and feasibility of, legislative reform.[75] Specifically in relation to the question whether the existence of a website is enough to assert jurisdiction, it could be objected, first, that courts have never had to deal directly with that question and therefore with the consequences arising out of an attempt to answer it. Secondly, even if courts had to deal with the question, their concern to make a pragmatic decision designed to achieve justice in the particular circumstances of the case makes them blind to the possible impact of their decision in the future. Thirdly, even if judges recognised the consequences of adopting existing jurisdictional

[74] Burk, above n. 24, paras. 25f. [75] Atiyah, above n. 52, 130ff.

doctrines in relation to the Internet, they as 'mere' judges have no choice but to uphold them. Are these objections valid?

The first objection to the moderate judicial approach may be that judges had the luxury of some indicators which supported their arguments for or against adjudicative jurisdiction and never had to answer directly the 'pure' question of whether the existence of a foreign website can justify the assertion of jurisdiction over the entity or person behind the site. Indeed, some judges have been at pains to stress that the case before them does not raise that very question. For example, in *Altavista*, the judge said:

> While this case raises some of the concerns, they are not, in the final analysis, dispositive. There is no issue of inconsistent regulation suddenly imposed on Web users without notice. There is no issue of parties being haled into the courts of a given jurisdiction solely by virtue of a Web-site, without meaningful notice that such an outcome was likely. Nor is there a great risk of chilling the Internet's 'participatory marketplace' by affirming jurisdiction here . . . This case does not reach the issue of whether any Web-activity, by anyone, absent commercial use, absent advertising and solicitation of both advertising and sales, absent a contract and sales and other contact with the forum state . . . would be sufficient to permit the assertion of jurisdiction over a foreign defendant.[76]

Nevertheless, it is misplaced to say that the judiciary has had the luxury of indicators or distinctions allowing them to make decisions according to traditional jurisdictional concepts, as if these were necessary and pre-existing. While the above-mentioned distinctions are no doubt based in reality, they are ultimately the result of judges' creativity. By creating them, judges have rejected the validity of even asking the 'pure' question whether the accessibility of a website, that is, *any* website, can justify the assertion of regulatory competence. This question is based upon a decision to treat all websites as a uniform phenomenon – a decision judges have implicitly rejected. When courts have decided not to exercise jurisdiction, as, for example, in *Bensusan Restaurant Corporation* v. *King*, it was because indicators pointing in favour of jurisdiction in other cases were absent rather than because the courts

[76] 960 F Supp 456, 463 (D Mass. 1997). See also *Heroes Inc.* v. *Heroes Foundation*, 958 F Supp 1, 5 (DDC 1996): 'Because the defendant's home page is not the only contact . . . the Court need not decide whether the defendant's home page by itself subjects the defendant to personal jurisdiction in the District.'

rejected the validity of the distinctions drawn.[77] Judges have not attempted to answer the question of whether the accessibility of *any* website is enough to assert jurisdiction. Furthermore, given the far-reaching consequences of asking the question, it is questionable whether it will or should be asked.

The second objection may be that a judge's concern to make a pragmatic decision designed to achieve justice in the particular circumstances of the case makes him or her blind to the possible impact of the decision in the future.[78] And, it may be argued, this short-sightedness will have particularly grave consequences where the currency of existing legal doctrines is profoundly challenged by social and economic change. Again, this objection is at least partially unmerited. Although some judges no doubt fail to appreciate the wider, long-term consequences of their decisions,[79] the very choice they have to make between two (or more) potentially applicable legal propositions is affected by comparing the consequences of adopting either. So judges have rejected the legal propositions that *no* website or *every* website justifies an assertion of jurisdiction, in favour of the proposition that *some* websites justify it, precisely because the future impact of the last proposition is more acceptable. It produces greater legal stability, and thus social and economic stability, than the others. Again, the example of *Playboy Enterprises Inc.* v. *Chuckleberry Publishing Inc.* illustrates this nicely. In explaining her choice to extend the injunction to the Internet, the judge said that the Internet deserves protection:

> However, this special protection does not extend to ignoring court orders and injunctions. If it did, injunctions would cease to have meaning and intellectual property would no longer be adequately protected. In the absence of enforcement, intellectual property law could easily be circumvented through the creation of Internet sites that permit the very distribution that has been enjoined. Our long-standing system of intellectual property protections has encouraged creative minds to be productive. Diluting those protections may discourage that creativity.[80]

[77] 937 F Supp 295, 301 (SDNY 1996), where the court distinguished rather than rejected the decision in *Compuserve* v. *Patterson*, 89 F 3d 1257 (6th Cir. 1996).

[78] Atiyah, above n. 52, 1251.

[79] See, for example, *Inset Systems Inc.* v. *Instruction Set Inc.* 937 F Supp 161 (D Conn. 1996), where the court held that advertising via the Internet is solicitation of a sufficiently repetitive nature to justify assertion of jurisdiction over the out-of-state defendants. See also *Maritz Inc.* v. *CyberGold Inc.*, 947 F Supp 1328 (ED Mo. 1996). Both decisions have been criticised for being too expansive; see above n. 61.

[80] 939 F Supp 1032, 1039f (SDNY 1996).

While the capacity of judges to evaluate correctly the relative viability of alternative legal propositions in the long run is limited (which incidentally is not peculiar to the judiciary), it must be remembered that 'actors in the legal process are not called upon to decide truths for all time, rather they must deal with a selection of competing legal positions in a limited context, though the outer boundary of relevant concerns may be vague ... Since no immutable conclusions are to be drawn, there is every justification for accepting the most rational solution available at the time.'[81] If judges were to attempt to decide immutable truths for all time, they could not be responsive to the peculiarities of particular times. They would have to reject any proposition which is in some way reflective of the particular background against which it is made.[82] The result would be broad and vague statements of law which could not answer the basic need for certainty that law is there to answer. So judicial reasoning may be short-sighted but this is, to a certain extent, neither peculiar to the judiciary nor undesirable.

The final objection may be that judges have no power to reject existing rules, even if they were persuaded of their inappropriateness in relation to the Internet. Along those lines, the judge in *Hearst Corp*. v. *Goldberger* said that, although 'some commentators ... believe a new body of jurisprudence is needed ... [on] the question of personal jurisdiction and the Internet ... [u]nless and until Congress ... enacts Internet specific jurisdictional legislation, however, the Court must employ ... existing jurisdictional statutes ... and analogize to presently existing, traditional, non-Internet personal jurisdiction case law'.[83]

However, this limitation on judicial power should not be overemphasised, as the judiciary does have the power and the obligation to limit or expand the application of existing rules if the context of the case demands it. Thus indirectly judges do pass judgment on the viability of the rules themselves. For example, in *Playboy*, an Italian company was alleged to have breached a fifteen-year-old injunction prohibiting it from distributing its *Playmen* glamour magazine in the US by reason of the fact that it was put on its website and so became accessible from the US. The judge rejected the argument by the Italian company that the

[81] Sinclair, above n. 31, 856.

[82] Peter Stein and John Shand, *Legal Values in Western Society* (Edinburgh: Edinburgh University Press, 1974), 26, noting, in the context of free speech, that law is 'finely attuned to the speech needs of a society at a particular time'.

[83] *Hearst Corp*. v. *Goldberger*, WL 97097 (SDNY 1997) 7.

injunction does not apply to the new medium of the Internet. She could have held the reverse; this would clearly have been an available option under the law. It would have amounted to saying that the Internet is such a radically new medium for publication and distribution that the old court order, and implicitly the law upon which it was based, cannot validly be applied to it. So courts could have, within their legitimate power, adopted the legal propositions either that no, or that every, website justifies an assertion of jurisdiction, both of which would indirectly amount to a rejection of the viability of existing jurisdictional concepts. They decided not to. The judiciary often has considerable power to reject indirectly existing rules if social and economic change renders them outdated; indeed, choosing one rule in preference to another cannot but entail the rejection of the latter rule.

So the moderate and incremental approach adopted by the judiciary cannot be attacked simply by saying that judges inevitably submitted to inherent judicial limitations and thus had no choice but to decide the way they did. The question is: what makes one rule more attractive than another in the eyes of a judge and thereby in the eyes of the legal system?

C. The best solution versus the least disruptive solution

Asserting that this moderate tradition-bound approach cannot be rejected as typically judicial, does not necessarily mean that it is good. Should not the preoccupation with legal tradition give way to a preparedness to effect as much legal change as is called for by an unbiased assessment of the workability of existing legal rules under the changed circumstances? Johnson and Post answered this question positively. Like many other scholars, they simply asked the question whether there is a better way to deal with the new phenomenon of the Internet than by using the existing jurisdictional regime – and there always is. In terms of the earlier discussion on legal reasoning, they reject subsumptive reasoning from pre-established rules and adopt a more forward-looking, goal-oriented type of reasoning. Johnson and Post's aim was to come up with the best and most efficient regulatory model available. This is a worthy goal, but unfortunately not easily reconcilable with the need for legal stability. By being so quick to reject the past jurisdictional regime[84]

[84] Their argument though is designed to retain existing broad regulatory objectives, and even attempts to find some continuity with past competence rules: 'We can *reconcile* the new law created in this space with current territoriality based legal systems by treating it as a distinct doctrine.' Johnson and Post, above n. 2, 1400f (emphasis added).

they became blind to the ways one could work within those very regimes. The judiciary has been much less ambitious. They have asked how existing rules could accommodate the new online phenomenon, regardless of whether they are the theoretically best possible rules. While this question seems inferior and more timid than the search for the ideal solution, its strength lies in its insistence on legal continuity. It reflects the law's resistance to anything but incremental change. Indeed, as the judiciary is an integral part of the legal regime, to view its decision in favour of the most tradition-bound position as a matter of free choice is illusory; it could not but search for the least disruptive legal solution available.

And this search is not peculiar to the judiciary. Even the legislature does not freely inquire into, and choose, the best possible regulatory option, regardless of the regulatory tradition and regardless of the extent of legal change the implementation of that option would require. The legislature's resistance to major change, despite its best efforts to effect change, is illustrated by the complaints which have surfaced frequently in relation to cyberspace regulation:

> Even the Clinton Administration's present effort to develop a vision for the information infrastructure ... remains captive to sectoral thinking and reactive tendencies ... [S]ome of the most time-consuming projects, like privacy and intellectual property remain focused on territorial borders and the transposition of status quo interests to cyberspace.[85]

These reactive tendencies are also exhibited in legislators' preferences in regard to the type of regulatory approach. Governments have often launched into the new field of cyberspace with the type of regulations with which they are familiar, and used to, from the offline world regardless of how well suited they are to cyberspace.[86] A classic example is the EC Directive on spam mail which prohibits the sending of

[85] Reidenberg, above n. 6, 923; see also *ibid*., 924, where the author notes, in relation to the EU omnibus approach to regulation, that it nevertheless 'tends to preserve important, yet evaporating, foundations based on territorial principles and subject matter distinctions'.

[86] This is not to say that more effective regulatory approaches are necessarily better, taking into account other values like personal autonomy or transparent governance. See, for example, Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501, where the author expresses concern that governments may eventually wake up to a new style of regulation much better suited to the online world.

unsolicited email in the absence of prior consent by the addressee, but has had little, if any, impact on the prevalence of spam.[87] Whatever the flaws of these regulatory attempts, they clearly illustrate how tradition-bound even the legislature is, seeking to retain the regulatory *status quo*. And the reason for this is not simply a failure, owing to incompetence or lack of insight, to rise to the challenge but lies in the very nature and function of law as a shield against instability and uncertainty.

So far the analysis has established how judges have been able to resurrect apparently doomed jurisdictional principles, allowing the law to evolve even at times of drastic social and economic changes. It has also been argued that the search for the least disruptive ruling to the new jurisdictional problems, while not the result of judicial shortcomings, is rather symptomatic of any legal regime's general resistance to major change. Legal argumentation which searches for the best regulatory options regardless of the regulatory tradition, while instructive through its emphasis on regulatory shortcomings, will not yield realistic and viable solutions.

5. Law as an engine of, or brake on, change

In times of dramatic social and economic change, such as produced by the online revolution, the focus tends to be on how law should respond to this change. Yet law is not simply reactive to external changes but is often itself an engine of, or less constructively a brake slowing, such change. The discussion below considers two arguments advanced against the viability of current competence regimes in the online age. Both arguments, it is contended, fail to take into account the active, although not necessarily proactive, role law plays in shaping society. Yet, this aspect of law lends further weight to the argument that incremental legal changes can often accommodate seemingly non-incremental social and economic changes.

[87] Directive on Privacy and Electronic Communications, 2002/58/EC, implemented in the UK by the Privacy and Electronic Communications (EC Directive) Regulations 2003. In 2005, spam, according to one estimate, still accounted for two-thirds of all emails. Office of Fair Trading, *Cross-Border Action to Tackle Spam* (3 November 2005), www.oft.gov.uk/News/Press+releases/2005/208-05.htm, further discussed in Chapter 7.

A. The floodgates argument

The new quantitative burden which traditional jurisdictional regimes are subjected to gives rise to a typical floodgates argument: the relatively complex jurisdictional regimes – tailored to an environment where most conduct and transactions are localised within a State – are unsustainable in the Internet age where transnational conduct is far from exceptional. Consequently, the judiciary's attempt to preserve traditional jurisdictional regimes is futile because these regimes cannot possibly cope with the innumerable disputes arising out of the millions of online transnational transactions.

This new quantitative jurisdiction problem has not attracted as much attention as the qualitative one. Nevertheless, the potential for a great increase in transnational disputes has featured as the factual background against which genuinely new jurisdictional issues are discussed. So Johnson and Post argue that the existence of a website is insufficient to assert regulatory power, mainly by appealing to the logical implication of that proposition, namely, worldwide legal exposure. But Lessig in turn evaluates this in light of the fact that there are millions of websites brewing endless transnational disputes. He then concludes:

> Cyberlaw will evolve to the extent that it is easier to develop this separate law than to work out the *endless* conflicts that the cross-border existences here will generate . . . The alternative is a revival of conflicts of law; but conflicts of law is dead – killed by a realism intended to save it. And without a usable body of law to deploy against it, a law of cyberspace will emerge as the simpler way to resolve the inevitable, and *repeated*, conflicts that cyberspace will raise.[88]

The significant increase in transnational conduct adds another dimension to the debate on the adequacy of traditional jurisdictional principles. Supposing there were a total of seven websites worldwide, any heated debate on the issue whether or not an assertion of jurisdiction can be based on the mere existence of a website would be hard to imagine. In the greater scheme of things, it would matter little whether or not all or any of these seven sites were subject to the jurisdiction of every State. Yet, even if one accepts that the amount of actual online activity is relevant to deciding how to resolve jurisdictional

[88] Lawrence Lessig, 'The Zones of Cyberspace' (1996) 48 *Stanford Law Review* 1403, 1407.

disputes, is Johnson and Post's vision of a flood of endless and repeated jurisdictional conflicts demanding radical legal changes justified? And are judges merely burying their heads in the sand when their rulings are not informed by this floodgates argument?[89]

Although there has been a general increase in jurisdictional disputes, appeals to floodgates arguments seem unjustified, especially in relation to those areas of law which provide yardsticks according to which people order their affairs, such as commercial law, as opposed to those areas of law which primarily come into operation only after the relevant event or conduct occurred, such as torts and criminal law.[90] Particularly in the world of commerce, law does not merely respond to behaviour, but also shapes it:

> greatest weight should be given to outcomes in the way of probable behavioral changes in respect of novel rulings, in those areas where it is particularly likely that people will explicitly ground their actions in the law as it is laid down, [such as t]ax law, insurance law, and conveyancing . . . [I]n such fields in which people and companies are expected to act after informing themselves, or being professionally advised, about the law, it is highly probable that the outcomes of rulings on the law will be behavior that either conforms to it or takes advantage of the opportunities offered by it or otherwise adjusts affairs and practices to allow for it.[91]

The effect of any legal ruling in these areas of law is to pre-empt many similar disputes. Decided cases are turned into risk-management strategies designed to minimise a business' or consumer's exposure to the same costly conflicts. For example, it has been said that:

> Financial institutions and merchants should reevaluate the trade-offs between an enhanced multi-jurisdictional marketing and transnational presence against the impact such presence may have on jurisdictional defenses. Participants in electronic commerce can take steps to minimize the risk of jurisdiction in a foreign forum by use of disclaimer or

[89] Courts tend to refer to the number of Internet users worldwide or the speed and efficiency of the Internet, if at all, in their introduction as a matter of the general background, without making this quantitative aspect an expressly stated reason for deciding one way or another. For example, *Playboy Enterprises Inc.* v. *Chuckleberry Publishing Inc.*, 939 F Supp 1032, 1036 (SDNY 1996); *ACLU* v. *Reno*, 929 F Supp 824, 831f (ED Pa 1996).

[90] But, even in those areas, the threat of *ex post* sanctions is intended to have some deterrent effect and actively to influence behavioural choices.

[91] Neil MacCormick, 'On Legal Decisions and Their Consequences: From Dewey to Dworkin' (1983) 58 *New York University Law Review* 239, 253f.

> otherwise conveying intended geographic limitations of the entity's service area and by limiting the interactive nature of their electronic contacts with forum residents, limiting their non-Internet contacts with the forum, and as an extreme measure, restricting access via the forum or by forum residents.[92]

Whether these strategies are desirable or not is not the issue at this point. What is noteworthy is the interactive relationship between law and commercial reality. As law is changing in response to a new commercial phenomenon, this phenomenon in turn responds to the law. This mutual adjustment of, or the closing of the gap between, law and commercial reality transforms a situation which might initially appear to require radical changes in the law into one which can be dealt with by adjustments of the law. Take, for example, consumers in the global electronic marketplace. As long as existing jurisdictional regimes are inefficient in dealing with transnational consumer disputes, it is unlikely that many of these disputes will occur because consumers are discouraged from entering into transnational transactions in the first place. Nevertheless, as some disputes arise, they put pressure on the traditional law. If the law governing these transactions adjusts by, for example, becoming simpler and more efficient, consumer confidence in electronic commerce will rise, resulting in more transactions, which in turn will put pressure on the legal regime to change yet again.[93] While this description of incremental legal change in response to commercial change and *vice versa* is no doubt oversimplified, it does serve to show the falsity of viewing the relationship between law and commercial reality as simply one-way, as well as the corresponding arguments for radical legal change based on this assumed one-way relationship.[94]

This description of the impact of law on consumer behaviour also proves that one should not too hastily accept generalised arguments to

[92] Thomas P. Vartanian, Robert H. Ledig and Lynn Bruneau, *21st Century of Money, Banking and Commerce* (Washington DC: Fried, Frank, Harris, Shriver & Jacobson, 1998), 623.

[93] Showing some of the characteristics of what is known as the snowballing phenomenon or network effects, described, for example, in Mark A. Lemley and David McGowan, 'Legal Implications of Network Economic Effects' (1998) 86 *California Law Review* 479.

[94] For example, those who argued that the law of copyright would need to be changed drastically in the age of the Internet or else the creation of copyright material will be stunted have already been proved wrong by the flexibility of owners of copyright material in adjusting to the new medium of the Internet and in making up for the legal shortfalls: Schlachter, above n. 17.

the effect that the Internet has removed all the factual assumptions upon which jurisdictional regimes have relied. For example, although the Internet seems to make transnational transactions as easy and cheap as domestic transactions, in fact the uncertainties and costs in case of dispute mean that, for all but the most low-value transactions, geographic distance is still an important consideration. This is a factual assumption upon which jurisdictional regimes can still rely.

B. The futility argument

Indeed, some background factual assumptions which the Internet has threatened are being reinvented within the new space. In the jurisdictional context, one of those assumptions is the existence of clear, recognisable, territorial borders, which do not appear to be even capable of existence in cyberspace. Yet, as legal regimes attempt to subsume the online world within them, physical boundaries are being superimposed on cyberspace. Already in the early case of *Playboy* v. *Chuckleberry* the judge ordered the defendant to refuse subscriptions from US customers in relation to its password-protected Internet service. She also said that its free Internet service must be shut down or made compliant with the injunction by requiring users to:

> acquire free passwords and user IDs in order to access the site. In this way, users residing in the United States can be filtered out and refused access. [Footnote] If technology cannot identify the country of origin of e-mail addresses, these passwords and user IDs should be sent by mail. Only in this way can the Court be assured that United States users are not accidentally permitted access to Playmen Lite.[95]

By making this order, the judge effectively said that she was not impressed by the futility argument, that is, the argument that laws based on geographic boundaries are not feasible on the Internet,[96] requiring the website operator to manipulate the architecture of the website so as to make it recognise territorial boundaries. As will be seen in later chapters, this very attitude has become standard, and has been

[95] *Playboy Enterprises Inc.* v. *Chuckleberry Publishing Inc.*, 939 F Supp 1032, 1044f (SDNY 1996).

[96] For example, Johnson and Post, above n. 2, 1372: 'efforts to control the flow of electronic information across physical borders – to map local regulation and physical boundaries onto Cyberspace – are likely to prove futile, at least in countries that hope to participate in global commerce.'

adopted in a variety of legal contexts by judges and legislators across the globe.

The order by the judge was defensible because it can be complied with, and it can be complied with because the Internet is not a static technical phenomenon incapable of changing in response to outside pressures and adjusting to regulatory objectives. As a man-made facility, the Internet is not immutable:

> There is no single architecture that is essential to the net's design. Net 95 [the Internet in the year 1995] is a set of features, or protocols, that constituted the net at one period of time. But nothing requires that these features, or protocols, always constitute the net as it always will be. And indeed, nothing in what we've seen in the last 2 years should lead us to think that it will.[97]

In the last decade, Internet software has become significantly more sophisticated; today online content providers have at their disposal software which allow them to recognise the geographic location of their visitors and exclude end-users from legally inhospitable States. So in fact the Internet is no longer quite the border-defying creature Johnson and Post took as their starting point.

Another point which emerges from the ruling is that substantive regulation need not be discarded if the underlying factual assumptions – upon which the traditional rules have relied and which the new technological or other development displaces – can be recreated. So, instead of the law changing in response to the new phenomenon, holding onto the legal *status quo* creates an incentive for the new phenomenon to make adjustments to fit the old law. The gap between law and the new environment is closed by manipulations of this environment to imitate the old one. In turn, this means that only minor rather than drastic legal reforms are needed. Whether such manipulations to suit the law are always a good thing may be questioned, but that it can and does occur in the online environment in respect of various legal contexts is beyond doubt.[98] The creation of borders in cyberspace is one example, and is examined in more depth in Chapter 7. Another classic example is the

[97] Lawrence Lessig, 'The Laws of Cyberspace – Draft 3' (1998), http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf, 8.

[98] Mayer, above n. 6, 35, Lessig, above n. 97 and above n. 86; Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 *Texas Law Review* 553. The most pervasive example is access restrictions, i.e. measures to reduce the easy accessibility of online material to everyone with an

new software available (and protected by law from attempts to circumvent it[99]) to counteract the ease with which copyright may be infringed in the digital online environment.

In summary, both the floodgates and the futility arguments take insufficient account of the two-way interactive relationship between law and society. The floodgates argument fails to acknowledge the impact of law, including its inadequacies, on rational market players. The futility argument does not take account of the dynamic nature of the Internet architecture which is clearly amenable to change in response to regulatory pressures. Both failures ultimately yield conclusions according to which drastic legal changes are necessary when in fact the regulatory gaps may be substantially narrower than is at first apparent.

C. The cautious way forward

In an ideal world, one could perhaps sit down and write new laws on a clean slate to fit changed circumstances perfectly – although perhaps in such an ideal world there would be no need for change in the first place. But we do not live in such a world, and so it is critical to understand legal change, and when and how it occurs, and let those insights inform arguments for law reform. This should not be understood as a fatalistic resignation to an immutable legal machinery with a life and a will of its own, but simply as a way of avoiding unrealistic legal propositions.

Once it is appreciated that drastic legal change does not fit squarely with the law's function to promote social and economic stability and certainty, it is clear that one cannot simply search for the best regulatory solutions no matter how such solutions fit into the existing legal framework. Correspondingly, there is an intrinsic value in holding onto existing legal rules and structures as far as possible, beyond the substantial value which the particular rule expresses and which may be less persuasive in new social and economic conditions. Legal argumentation

Internet connection. Such restrictions are adopted for various reasons, including to protect the commercial value of the information, to protect children from unsuitable material, to prevent legal exposure to the laws of inhospitable States or to gain regulatory favours. At times, the legislation specifically demands such access restrictions, e.g. under the US Communication Decency Act (although largely declared unconstitutional in *Reno* v. *ACLU*, 521 US 844 (1997)), a provider of pornography had a defence to the charge of displaying indecent material in cyberspace provided he adopted measures for screening out children.

[99] See, for example, Art. 6 of the Copyright Directive, 2001/29/EC, or Title I of the US Digital Millennium Copyright Act 1998.

must be conservative and cautious particularly in relation to legal issues arising out of a phenomenon as revolutionary as the Internet; in respect of more gradual changes conservatism tends to be assumed as the natural mode. There are no alternatives to the concept of *stare decisis* in its widest sense. Legal argumentation must focus on retaining, reshaping and redesigning rules, and searching for ways in which these can be preserved. No doubt these ways can be more easily discovered in the practical context in which the rules operate and in which their defects and strengths are more easily discernible. Focus on this practical context tends also to reveal how urgent the need for legal change really is. So, in addition to searching for what may be perceived as the best solutions, the inquiry must also focus on the least disruptive solutions. Their shortcomings in efficiency they make up through providing continuity and certainty.

Finally, even in the trademark-versus-domain-name context, this conservative approach has, seemingly against all the odds, allowed traditional national law to evolve to accommodate transnational cyberspace.[100] But there is no doubt that the judicial solutions found are far from ideal. Under the *Zippo* test, it is only non-commercial websites, or commercial websites that avoid trading in the State where a clash with locally registered trademarks could occur, that can escape the regulatory clutches of the foreign State. The price to be paid for the retention of traditional trademark law is high: it discourages use of the Internet to its full potential by encouraging territorial restrictions on websites and limiting their commercial usage. A small *local* business in the real world is safest to stay a small *local* business online, and that seems unfortunate. Also, one might wonder how easy it actually is to legally localise a website under the targeting or directing test: is attracting one customer from a certain locality enough to hold that the site carries on business there? If not, how many customers would be needed to come to that conclusion? What if the site has no customers at all but many visitors from a certain locality? Is the 'targeting' test a satisfactory solution to retaining territorially based laws in respect of seemingly non-territorial online activity? This is what the inquiry turns to now.

[100] Note that this national solution runs parallel to some regulatory development at the international level, most notably, in the trademark/domain names context, the role of the Internet Corporation for Assigned Names and Numbers (ICANN) as overall supervisor of the creation and allocation of domain names and as adjudicator with respect of certain registrations under its Uniform Dispute Resolution Policy (1998). See further Chapter 7, nn. 41–50, and the accompanying text.

3

The tipping point in law

1. Contract law: unaffected by online transnationality?

Unlike trademark law, contract law is one area in which the transnational nature of the Internet could pose no more than a small problem – at least in theory. Because, at least in theory, in a transnational contract it is the parties who decide who is going to regulate them: they decide which court should adjudicate their dispute (choice-of-forum clause) and which law should govern their dispute (choice-of-law clause). The contractual parties, exercising their contractual autonomy, create the link to found regulatory competence. In theory, the location of the parties, the location where the contract was entered into, the location of its performance or any breach thereof do not matter. All that matters is which legal system the parties to the contract have chosen, and therefore the non-territorial nature of the Internet and online activity is quite irrelevant.[1]

That is the theory. The reality is more complex. Contractual parties not infrequently fail to make those choices which link them to one legal system rather than another.[2] More critically, contractual autonomy is not something which exists outside and beyond legal systems. On the contrary, it is created or, at the very least, must be recognised and

[1] See, for example, English private international law, as discussed in J. G. Collier, *Conflict of Laws* (3rd edn, Cambridge: Cambridge University Press, 2001), 193.

[2] Ulrich Magnus and Peter Mankowski, *Joint Response to the Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument and its Modernisation COM(2002) 654 final* (2003), 2, http://ec.europa.eu/justice_home/news/consulting_public/rome_i/news_summary_rome1_en.htm, where the authors note that, for example, in all German cases dealing with international contract law decided in 2000, in only one-fifth of them had an express choice-of-law clause been included in the contract. Equally, many websites do not seem to include choice-of-law and choice-of-forum clauses in their terms and conditions. On the other hand, arbitration clauses appear very popular amongst US Internet businesses: Elizabeth G. Thornburg, 'Going Private: Technology, Due Process, and Internet Dispute Resolution' (2000) 34 *UC Davis Law Review* 151, 179ff.

enforced by States.[3] And, while most legal systems are committed to contractual autonomy generally,[4] they invariably impose some restrictions on it, refusing, for example, to recognise contractual agreements the performance of which would involve an illegality. Also, any term purporting to exclude a State's criminal or other public law would find little favour anywhere.[5] This is significant in the transnational context, as the parties' choice of the legal system which they wish to govern their contract may not be recognised and may be partly or wholly replaced with a court or substantive body of law which appears more closely connected to the contract and the parties.[6] And, as 'closely connected' (or other tests used to replace the contractually chosen legal system) is invariably determined by reference to location-oriented factors,[7] the non-territorial Internet becomes after all problematic – problematic in the same way as in other legal contexts.

One pertinent question in the contractual context is whether – in light of the difficulty of administering territorial-centric links in respect of the

[3] On a liberal contractualist perspective of law and regulation, private agreements precede law and it is the State's function to recognise them. Eilis Ferran, *Company Law and Corporate Finance* (Oxford: Oxford University Press, 1999), 10ff.

[4] This is, for example, reflected in the fact that – although the attempt by the Hague Conference on Private International Law comprehensively to harmonise jurisdictional principles in civil and commercial matters was unsuccessful – agreement could be achieved on choice-of-court agreements: Convention on Choice of Court Agreements (2005), www.hcch.net/index_en.php?act=conventions.text&cid=98/. In the EU, see Art. 23 of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001; and Art. 3 (Freedom of Choice) of the Rome Convention on the Law Applicable to Contractual Obligations (1998). For the traditional English common law position, see e.g. *Vita Food Products Inc.* v. *Unus Shipping Co.* [1939] AC 277 (PC).

[5] It is not within the power of individuals to exclude the application of criminal or public laws to them by a clause stating, for example: 'The parties to the contract shall not be subject to the criminal laws of England.'

[6] See e.g. Art. 7 (Mandatory Rules) of the Rome Convention on the Law Applicable to Contractual Obligations (1980).

[7] For example, in England and Wales, reg. 9 of the Unfair Terms in Consumer Contracts Regulations 1999 states: 'These Regulations apply notwithstanding any contract term which applies . . . the law of a non-Member State, if the contract has *a close connection with the territory* of the Member States' (emphasis added). Art. 4 of the Rome Convention on the Law Applicable to Contractual Obligations (1980) provides that 'a contract shall be governed by the law of the country with which it is most closely connected', and then defines the close connection by reference to the location of the characteristic performance. Interestingly, this rule has been described as coming 'close to being a non-rule' for all its flexibility. Magnus and Mankowski, above n. 2, 19, supporting the proposed cautious evolutionary development of the Rome Convention.

non-territorial cyberspace – it may not be better to give greater weight to contractual choice and limit the exceptions to bare necessities.[8] For online businesses and even their customers, being certain of the relevant contract law would remove at least one of the many unknowns.[9] Yet, so far, States have firmly resisted changing their existing stance on contractual autonomy – as, for example, in the EU with a strong consumer protection tradition. Some have argued that this is regrettable as there are other factors – apart from the difficulty of administering location-sensitive jurisdictional exceptions – that suggest that the online market has shifted the traditional unequal bargaining position between businesses and consumers back in favour of consumers.[10] Many online businesses are rather small and not like the traditional multinational giants. Thus, on the one hand, they may be less likely to enter into standard-form contracts with consumers and, on the other hand, they may be less able to absorb the cost of having to comply with all the laws of the States of their customers. Also, the availability of tools such as price-value-comparison sites and feedback requirements,[11] and greater

[8] For example, Bradford L. Smith, 'The Third Industrial Revolution: Law and Policy for the Internet' (2000) 282 *Recueil des Cours* 229, 332; International Chamber of Commerce, *Jurisdiction and Applicable Law in Electronic Commerce* (6 June 2001), www.iccwbo.org/home/statements_rules/statements/2001/jurisdiction_and_applicable_law.asp. There may of course be substantial arguments as to what amounts to such necessities.

[9] There is a significant body of both private and public law which is applicable to commercial activity and which cannot be excluded contractually.

[10] American Bar Association, 'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf, 32ff, 93ff; Denis T. Rice, '2001: A Cyberspace Odyssey Through US and EU Internet Jurisdiction Over E-Commerce' (2001) 661 *PLI/Pat* 421, 450ff; in favour of contractual autonomy in consumer transactions, see Yahoo! Europe, *Comments on the Green Paper on a 'Rome 1 Regulation'* (2003), http://ec.europa.eu/justice_home/news/consulting public/rome_i/news_summary_rome1_en.htm. For a defence of continued consumer protection, see, for example, Joakim S. T. Oren, 'International Jurisdiction over Consumer Contracts in e-Europe' (2003) 52 *International and Comparative Law Quarterly* 665, 669–72, noting in particular the pre-payment requirement for consumers in most e-commerce transactions. Also, OECD, *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999), para. VI. Generally, on the need for public measures to protect the consumer in the transnational online environment, see e.g. OECD, *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (2003), www.oecd.org/dataoecd/24/33/2956464.pdf.

[11] For example, Amazon competes for customers with other 'market participants', all of which also rely on feedback from previous customers as vouchers for their respectability.

choice between suppliers, empowers consumers *vis-à-vis* online businesses. In auction scenarios, where the seller is also often just a 'consumer', it is unclear whether traditional consumer protection provisions are, or should be, applicable. The competence questions considered below feed into this wider debate on substantive contract law in the online world.

The peculiarities of the Internet have been given their due in law reforms in the EU[12] and elsewhere. However, the focus has been more on how traditional legal protections can be retained than on whether they should be retained. For example, the new consumer exception to choice-of-forum clauses, discussed below, is designed to retain existing protections and accommodate the relative territorial insensitivity of cyberspace. The old has been adapted and fine-tuned to fit the new. But how helpful are these exceptions really? Building on the previous chapter, this chapter examines the fine-tuning process of traditional location-focused links to suit the Internet as well as an alternative to it. It shows the limits of incremental legal developments, and why, at least long-term, tinkering with existing territorial tests cannot possibly provide fair and efficient regulatory solutions to transnational activity.

2. The tipping point

A. *Evolution of law versus the tipping point*

The central argument in this chapter is that there comes a tipping point, when the finely tuned rules rely on such subtle distinctions and minor factual variations that they become unworkable – unworkable because they can deliver neither overall consistency (and thus formal justice) nor quick and easily predictable results (and thus efficiency). Paradoxically, the desire for certainty and predictability, leading to a strong preference for incremental legal change, sometimes shapes rules which defy the very aim which inspired them and thus ultimately create a need for more radical legal change. This shines through the comment that 'conflicts of law is dead – killed by a realism intended to save it ... [C]yberspace [law] will emerge as the simpler way to resolve the inevitable, and repeated, conflicts that cyberspace will raise'.[13] Whether the radical

[12] There are quite a few new EC Directives specifically aimed at protecting the online consumer, such as the Distance Selling Directive, 97/7/EC, the Electronic Commerce Directive, 2000/31/EC, and the Directive on Privacy and Electronic Communications, 2002/58/EC.

[13] Lawrence Lessig, 'The Zones of Cyberspace' (1996) 48 *Stanford Law Review* 1403, 1407.

change will come in this particular form or not, it is beyond doubt that law sometimes tips, just like other natural, ideological and social phenomena. The idea of the tipping point (or the straw that broke the camel's back) has been poignantly explained as follows:

> It wasn't much colder on the morning of his first snowfall than it had been the evening before . . . Almost nothing had changed . . . yet . . . everything had changed. Rain had become something entirely different. Snow! We are all, at heart, gradualists, our expectations set by the steady passage of time. But the world of the Tipping Point is a place where the unexpected becomes expected, where radical change is more than possibility. It is – contrary to all our expectations – a certainty.[14]

The argument in this chapter is that law too sometimes tips and appears to move towards the tipping point on the regulatory competence front.

Yet, this movement towards more sophisticated, fine-tuned rules is not an inevitable product of legal adjustments to the increasing transnationality, albeit the most rationally defensible route. This chapter contrasts the jurisdictional rules in private matters with those in criminal matters, highlighting an alternative answer to essentially the same question. This comparison makes it clear that the refinement movement is much stronger and sustained in the private context, although even in criminal matters there have been some similar adaptations in response to globalisation.[15] Yet, the end results – shaped by strongly divergent considerations – look very different. Ultimately, the comparison between competence rules in private and public matters puts into sharp focus their relative advantages and disadvantages,[16] as well as their intrinsic unsuitability in a world less restricted by distance. There can be no doubt: the Internet makes any rule – that makes the location of an activity the criterion for deciding what belongs to whom[17] – more and more difficult to administer and in the

[14] Malcolm Gladwell, *The Tipping Point* (London: Abacus, 2001), 13f.

[15] F. A. Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recueil des Cours* 1, 18f, where Mann comments on the many parallels in the doctrinal developments in respect of private and public law: 'so remarkable and striking a coincidence is likely to be the symptom of a deep-rooted doctrinal link.'

[16] These divergent developments in respect of transnational private and public law incidentally also show that the need for incremental adjustment to legal rules, as discussed in Chapter 2, cannot entirely account for how these rules actually evolve.

[17] The terminology of 'belonging' has been used in the jurisdictional context, for example, by Mann, above n. 15, 44f, where he argues that public international lawyers should, just like their private counterparts, 'ask whether the legally relevant facts are such that they "belong" to this or that jurisdiction.'

long-term unsustainable. Long-term, it is a certainty that the rules will tip in favour of non-territorial rules.[18] Short-term, greater recognition of contractual choice may ameliorate some problems.

B. Substantive justice versus formal justice

In traditional jurisprudential terms, this chapter concerns the increasing conflict between the demands of substantive justice and those of formal justice in the allocation of competence over global online activity. The Internet has had a dual impact on transnational activity in the context of existing jurisdictional rules. First, there is more transnational activity. Secondly, much of that transnational activity impacts on many more States than previous transnational activity: as every website can be accessed anywhere, they affect many States to such a degree as would give each State a *prima facie* stake and regulatory interest in them. Most online events are not just transnational but multinational.[19] This second aspect has led, as discussed in the previous chapter, to an adaptation of existing jurisdiction rules in private matters. They have been fine-tuned to remain as effective vehicles for choosing the worthiest of all would-be regulators. In other words, the fine-tuning (always designed to protect legal continuity and certainty) is, in the particular context of regulatory competence, designed to respond to the demands of substantive justice: the demands of individuals not to be exposed to the law and court processes of every State and, in particular, those with which they have had only minimal fortuitous connections, and also the demands of States to regulate those foreign activities which have a significant impact on their inhabitants. This seems rather unobjectionable.

The problem is that, while those finely tuned rules may meet the demands of substantive justice, they increasingly fail those of formal justice, namely, overall consistency or the requirement to treat like cases alike, and different cases differently. Briefly, one may distinguish:

> between specific conceptions of justice and the concept of justice. The difference is that the concept of justice is abstract and formal; the

[18] As discussed in Chapter 1, abandoning territoriality partly or wholly cannot but have major ramifications for the concept of the State which is its personification, the embodiment of the main organising principle of law and order on our globe.

[19] The two points broadly correspond to the distinction drawn in Chapter 2 between the quantitative and qualitative changes triggered by the Internet. Similarly, it corresponds to the eggs story in Chapter 1 concerning, first, the rise of new colour variations and, secondly, the rise of non-primary coloured eggs *per se*.

> requirement of formal justice is that we treat like cases alike, and different cases differently, and give to everyone his due; what various conceptions of justice supply is different sets of principles and/or rules in light of which to determine when cases are materially similar and when they are materially different; what is each person's due.[20]

What is illustrated below is that the desire to provide fair and just results, at least in the context of private transnational events, increasingly produces principles and doctrines which are so broad and factually specific that formal justice or consistency cannot be retained. Or, to put it another way, it is often difficult to explain why cases which seem and are *in fact* very similar are *in law* treated as materially different. The jurisdictional rules increasingly rely on minor factual differences to justify a materially different treatment in law, inevitably leading to inconsistencies. The argument is that these inconsistent decisions are not simply one-off errors, but systemic problems given the character of the rules. The rules are such that they cannot possibly yield certain and consistent results. In illustrating this, the focus shall not be on decisions which have in retrospect been regarded as wrong. Rather, even when judges get it right and apply the right rules to the right cases, the case law as a whole often proves them wrong.

As consistency goes, so arbitrariness comes, which is problematic beyond the practical problems to which it gives rise, such as the inability of individuals to order their affairs in accordance with the law. It is beyond argument, as MacCormick puts it, that it is:

> a fundamental principle that human beings ought to be rational rather than arbitrary in the conduct of their public and social affairs (spontaneity and a kind of arbitrariness have a welcome part to play in private activities and relations . . .). To somebody who disputes that principle with me, I can indeed resort only to a Humean argument: our society is either organized according to that value of rationality or it is not, and I cannot contemplate without revulsion the uncertainty and insecurity of an arbitrarily run society, in which decisions of all kinds are settled on somebody's whim or caprice of the moment.[21]

[20] Neil MacCormick, *Legal Reasoning and Legal Theory* (first published 1978, Oxford: Oxford University Press, 1994), 73 (footnotes omitted). See e.g. Recital 11 of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001, which stresses the importance of predictability.

[21] *Ibid.*, 76f. See also Hans Kelsen, *General Theory of Law and States* (Cambridge, MA: Harvard University Press, 1946), 14, where he states: '"Justice" in this sense means

Also, the failure to comply with the demands of formal justice overshadows any success on the substantive justice front. Any fair and just outcome must be weighed against the unpredictability and indeterminacy of the many borderline cases, and the wider consequences of having too complex rules govern a highly common phenomenon.

This brings us to another point: the problem of highly refined rules is exacerbated by the drastic increase of transnational activity – a reality which demands simpler and not more complex legal rules.[22] Sometimes, a refined legal regime, although born out of a desire to accommodate the new reality, cannot accommodate the very reality which inspired it. The evolution of the negligence action and its inadequacy in relation to car accidents is a prime example of a modernised legal doctrine which proved to be too inefficient to deal with the very scenario out of which it was born: 'Truly, if the highway created the negligence law of the 19th century, the highway of the 20th has doomed it to eventual oblivion.'[23] It shows that the sophistication of a doctrine can be problematic when the number of cases which attract its operation increases drastically. So, the very virtues of the negligence action, namely, its all-encompassing broadness and its fairness, reflecting subtle fault variations, contributed to its partial downfall: 'the wisdom of discarding strict liability for highway accidents seems less obvious today since the advent of the motor car than it was in the days of more tranquil traffic a

legality: it is "just" for a general rule to be actually applied in all cases where, according to its content, this rule should be applied. It is "unjust" for it to be applied in one case and not in another similar case. And this seems "unjust" without regard to the value of the general rule, the application of which is under consideration.'

[22] Ideally, consumers or businesses should not as a rule be better off internalising the loss arising e.g. from a breach of contract than enforcing what would be their legitimate rights. Rules which are workable only because they are too inefficient to be invoked seem in the long term highly unsatisfactory. Cf. Magnus and Mankowski, above n. 2, 24, arguing that the law should be seen in light of the fact that often the consumer 'internalises his losses and refrains himself from doing future business with the enterprise in question, putting its name on a "mental blacklist". Hence the probability that the enterprise will ever have to face the realisation of the *Rechtsanwendungsrisiko* effectively is rather low.'

[23] John G. Fleming, *The Law of Torts* (9th edn, Sydney: LBC Information Services, 1998), 25. In the context of competence, for example, the technique of statutory interpretation which dominated conflicts of law for five centuries was ultimately abandoned because it 'had become so complicated with divergent scholastic distinctions . . . that confused masters left their readers more confused': Hessel E. Yntema, 'The Historic Bases of Private International Law' (1953) 2 *American Journal of Comparative Law* 297, 304. Also discussed by F. A. Mann, 'The Doctrine of International Jurisdiction Revisited After Twenty Years' (1984) 186 *Recueil des Cours* 9, 27.

century ago ... Subsequent experience ... far surpassing the wildest fears, has seriously challenged the claim of fault liability as an adequate solution.'[24] The law dealing with traffic accidents tipped in favour of compulsory third-party insurance and no-fault compensation: 'without liability insurance the tort system would long ago have collapsed under the weight of the demands put on it and been replaced by an alternative, and perhaps more efficient, system of accident compensation.'[25] The development of the negligence action in relation to car accidents supports the main argument made here in respect of some competence rules: legal doctrines which seek to attain fairness and substantive justice through a wide, all-encompassing, highly fact-specific test may end up being less fair than a cruder but simpler and more certain test.

Such a test exists in respect of criminal matters. In many ways, the jurisdictional rules relating to transnational online crimes possess the exact opposite vices and virtues to those relating to civil matters. Although they are not plagued by concerns for formal justice, they move towards their own tipping point: they cannot provide *substantively fair* outcomes, moving swiftly towards a might-over-right approach which is unsatisfactory for both individuals and States.

3. The evolution of jurisdictional rules in private cases

A. Adjudicative jurisdiction in consumer contracts: no gain without pain

In private actions, a court has the right to adjudicate a dispute if it has personal jurisdiction over the defendant.[26] Traditionally – and this is still commonly the basic position to found personal jurisdiction – the defendant must be present or domiciled in the territory.[27] If not, the plaintiff has to go to the defendant's State to bring the action. This position has both moral and practical merits: as it is the plaintiff who has a complaint, it seems *prima facie* reasonable to expect him to go to

[24] Fleming, above n. 23, 25. [25] *Ibid.*, 13.

[26] Alternatively, *in rem* jurisdiction allows actions to be brought against ships or aircraft or more recently, in the US, against domain names under the Anticybersquatting Consumer Protection Act of 1999.

[27] 'Presence' is sufficient under English common law: *Emanuel* v. *Symon* [1908] 1 KB 302 and *Adams* v. *Cape Industries plc* [1990] Ch 433 (CA). Under Art. 2(1) of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001, the defendant must be sued in his place of domicile. See also *Kleinwort Benson* v. *Glasgow* [1999] 1 AC 153, 163f.

the defendant's State. Also, the presence of the defendant within the territory where the dispute is heard ensures that any judgment can be enforced against him or his property. In the contractual context, this general position has long been modified by the rule that a defendant may be sued in the court to which he has submitted through a contractual term, quite regardless of the parties' location.[28]

So, under both the general and the contractual rule, a plaintiff may have to go to a foreign court to be recompensed for a wrong done to him. The greater practical difficulties and legal uncertainties inherent in litigating abroad often mean that, especially concerning low-value transactions, being abroad effectively insulates the defendant from liability. This seems unfair if it was the defendant who actively sought the business in the plaintiff's State. Not surprisingly, rising numbers of transnational consumer transactions have led to the introduction of exceptions to both the general and the contractual positions.

One such exception was Article 13(3) of the Brussels Convention, which allowed a consumer to sue a foreign business in the former's home State whenever 'the contract was preceded by a specific invitation addressed to him or by advertising and the consumer took in that State the steps necessary for the conclusion of the contract'.[29] In *Rayner* v. *Davies*, the English Court of Appeal held that the critical question in

[28] See e.g. Art. 23 of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001. For England and Wales, see r. 6.15 of the Civil Procedure Rules 1998, according to which service out of jurisdiction may be permitted in respect of a contractual dispute, if the contract contains a term to the effect that the court shall have jurisdiction to hear and determine any action in respect of the contract. *British Aeropace plc* v. *Dee Howard Co.* [1993] 1 Ll R 368. For the US position, see below n. 42 and §32 of the US Restatement (Second) of Conflict of Laws (1971).

[29] Art. 13(3) of the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (1968): 'In proceedings concerning a contract concluded by a . . . consumer, jurisdiction shall be determined by this Section . . . if it is . . . (3) any other contract for the supply of goods or . . . services, and (a) in the State of the consumer's domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising and (b) the consumer took in that State the steps necessary for the conclusion of the contract.' The same rule still applies in respect of applicable law (see Art. 5 of the Rome Convention on the Law Applicable to Contractual Obligations (1980)), but is currently being reformed. See European Commission, *Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument and its Modernisation*, COM(2002) 654 final; and *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations*, COM(2005) 650 final.

respect of Article 13(3) was, who invited whom to do business.[30] Did the business leave its territory to seek the consumer on foreign shores, or was it the consumer who made the effort to find the foreign business at its home? In other words, where can the parties legitimately, given all the circumstances, expect to have to defend proceedings? Quite simply, an essentially local business need not fear being haled into a foreign court just because a foreign consumer knocks on its door.

Although this rule no doubt could have stood the test of time, it has been replaced by Article 15(1)(c) of the new EC Jurisdiction Regulation to cater specifically for the Internet. Under the new test, a consumer can sue at home[31] whenever the defendant had 'directed' his online business activities to the consumer's State.[32] This 'directing' test clearly encapsulates in a broader and perhaps less technology-specific way the same idea as the previous 'invitation' test: who was the instigator of the transaction? Who sought whom? Some argue that, by going online, a business necessarily seeks consumers from everywhere; but it could equally be argued that, by opening a real shop, a business seeks custom from everywhere. In the end, everything is accessible from everywhere – even the real shop. Yet, clearly some shops are more accessible to consumers

[30] [2002] EWCA Civ 1880, para. 26.

[31] Art. 16 of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001: 'A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts of the place where the consumer is domiciled. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled . . .'

[32] Art. 15(1)(c) of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001: 'In matters relating to a contract concluded by a . . . consumer . . . jurisdiction shall be determined by this Section . . . if (c) . . . the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.' This Article was hotly disputed; for the various stages preceding its adoption, see Oren, above n. 10, 679ff. More generally on the uncertainties in respect of the test's interpretation, see M. Foss and L. A. Bygrave, 'International Consumer Purchases through the Internet: Jurisdictional Issues Pursuant to European Law' (2000) 8 *International Journal of Law and Information Technology* 99; Ksenija Vasiljeva, '1968 Brussels Convention and EU Council Regulation No. 44/2001: Jurisdiction in Consumer Contracts Concluded Online' (2004) 10 *European Law Journal* 123. On the relationship of the Regulation with the country-of-origin rule in the Electronic Commerce Directive, 2000/31/EC (discussed in Chapter 5), see e.g. Peter Stone, 'Internet Consumer Contracts and European Private International Law' (2000) 9 *Information and Communications Technology Law* 5.

from certain countries: a real shop in Greece is more easily accessible to consumers in Greece. And the same reasoning can be applied to the Internet: certain websites are simply more easily accessible to certain consumers because of, for example, the products offered, language, advertising or currency, in short because the business 'directed' the site at the consumers of a certain State.

The 'directing' test is strikingly similar to the US 'targeting' test to establish personal jurisdiction. If this similarity were to be acknowledged, the EU could benefit from the large body of jurisprudence which has developed around the US test – particularly in respect of online scenarios. Yet, there has been strong resistance to such suggestions. The European Commission – although initially endorsing US concepts in respect of the directing test – later forcefully rejected any such American influence in response to the Parliament's proposal[33] to define 'directing' further and include, for example, any ring-fencing attempts of the online business within the deliberations. In a joint statement with the European Council, it noted: 'The definition is based on the essentially American concept of business activity as a general connecting factor determining jurisdiction, whereas that concept is quite foreign to the approach taken by the Regulation.'[34] Yet, they have never offered a convincing alternative interpretation, and have simply asserted that the existence of a consumer contract provides evidence of such 'directing'.[35] But, as Article 15 will only ever be invoked if the dispute in question concerns a consumer contract, the 'directing' test within the Article 15 would – on the Commission's interpretation – always be

[33] Amendment 37 (OJ C146/98, 2001) to the Proposal for a Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (OJ C376/17, 1999).

[34] Amended Proposal for a Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (OJ 062 E, 27.2.2001 P. 0243–0275), para. 2.2.2.

[35] *Ibid.*, which continues: 'the very existence of such a contract would seem to be clear indication that the supplier of the goods or services has directed his activities towards the state where the consumer is domiciled.' See also Joint Council and the Commission Statements (14 December 2000), 5, http://register.consilium.eu.int/pdf/en/00/st14/14139en0.pdf: 'The Council and the Commission point out in this connection that for Article 15(1)(c) to be applicable it is not sufficient for an undertaking to target its activities at the Member State of the consumer's residence, or at a number of Member States including that Member State; a contract must also be concluded within the framework of its activities.' More recently, in the context of applicable law, see *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations*, COM(2005) 650 final, para. 4.2, discussion on Art. 5.

satisfied. In other words, one may as well dispense with the directing test.[36] As this interpretation simply does not make sense, it would be more constructive to understand the similarities between the US and EU rules neither as coincidental nor as copycat attempts, but simply as the logical, rationally defensible, jurisdictional response to rising transnationality.[37]

The general maxim of substantive justice which underlies both the 'targeting' and the 'directing' tests (as well as the previous 'invitation' test) is simple: no gain without pain. If a business purposefully seeks custom from a particular State and profits from that custom (as evidenced by repeated contacts), it is also fair to subject that business to the court procedures (and often also the substantive laws) of that State. As is shown below, this general maxim of substantive justice has remained the same over the decades and perhaps even centuries; what has changed are the ways of transacting transnationally and with them the more specific rules which seek to implement the no-gain-without-pain maxim. The argument – made below by reference to US personal jurisdiction case law – is that this implementation is becoming increasingly unsatisfactory from a formal justice perspective. And this criticism applies equally to the EU 'directing' adaptation.

Before turning to these US developments, it must be stressed that in the US – with a strong contractual autonomy tradition – the 'targeting' test is not used to override a contractually chosen forum and applicable law in consumer contracts,[38] but rather as a personal jurisdiction test applied in non-contractual cases as well as in contractual cases where the parties have not made a contractual choice. This difference in the field of application cannot detract from the common considerations underlying

[36] Frederic Debussere, 'International Jurisdiction over E-Consumer Contracts in the European Union: Quid Novi Sub Sole?' (2002) 10 *International Journal of Law and Information Technology* 344, 357ff. See also Oren, above n. 10, 682f.

[37] This explains why it has also been adopted in relation to other areas of law, such as trademark law, in various jurisdictions; see Chapter 2, n. 67. See also Hague Conference on Private International Law (Catherine Kessedjian), *Electronic Commerce and International Jurisdiction*, Prel. Doc. No. 12 (2000), 6f. By the same token, attempts to apply traditional highly specific rules, such as the postal acceptance rule, to determine where an online contract was entered into, are invariably highly unsatisfactory, and should be replaced by tests less focused on the technological processes and more on the general context of the transaction.

[38] *Carnival Cruise Lines Inc.* v. *Shute*, 499 US 585 (1991) and *Haynsworth* v. *The Corporation*, 121 F 3d 956 (5th Cir. 1997). On the difference between Europe and the US, see also ABA, above n. 10, 87ff.

both tests and their common flaws, but does have minor ramifications for its interpretation and the types of contacts validly used to establish them.[39]

B. Pre-Internet refinements

The refinement process of jurisdictional rules in the private sphere is nowhere better illustrated than the US rules on adjudicative jurisdiction.[40] There, the question of whether a court can assume personal jurisdiction over a defendant and adjudicate a dispute has moved from a simple inquiry, relying on relatively clear-cut, objective facts, into a much more elaborate balancing approach, often depending on innumerable subjective value judgments. While most of these developments were in response to the increase of transnational interactivity long before the Internet era, the online phenomenon has added yet another layer of subtleties.

The turning point in the US came in 1945 when the US Supreme Court in *International Shoe Co*. v. *Washington*,[41] in recognition of the increased mobility of society, abandoned the requirement that the defendant must be physically present in the jurisdiction for the court to assume jurisdiction *in personam*.[42] Although this may not appear to

[39] In non-contractual cases, such as trademark cases, unlike contractual disputes, the existence of even a single contract with forum residents can be and has been used as evidence for targeting: addressed by Oren, above n. 10, 684ff, where the author cites the difference of the field of application and the US preoccupation with the 'due process' requirement as reasons why 'the US approach may contribute with some helpful guidelines, but must not be applied in any further extent than is justified by the specific circumstances in the different disputes'. In the view of the author, the differences between the two regimes are overstated.

[40] While most of the case law has developed in response to disputes arising between residents of states within the US rather than truly transnational disputes, and are preoccupied by the Fourteenth Amendment to the US Constitution requiring 'due process', neither of these two aspects detracts from the fact that these decisions constitute a response to ever increasing cross-border activity.

[41] 326 US 310 (1945). For a comprehensive overview of the cases since then with special focus on online cases, see ABA, above n. 38, 39ff. See also Sam Puathasnanon, 'Cyberspace and Personal Jurisdiction: The Problem of Using Internet Contacts to Establish Minimum Contacts' (1998) 31 *Loyola of Los Angeles Law Review* 691; Allan R. Stein, 'The Unexceptional Problem of Jurisdiction in Cyberspace' (1998) 32 *The International Lawyer* 1167, 1169ff, where the author describes the change as a move from a territorial basis of jurisdiction to a 'neo-territorial' basis.

[42] *Pennoyer* v. *Neff*, 95 US 714 (1887), where it was held that a State could not subject non-residents to the jurisdiction of its courts unless they were served with process within its

be such a major step, in fact it was. It meant that courts would sometimes exercise adjudicative jurisdiction even in the absence of enforcement jurisdiction. Incidentally, this shift is likely to have accelerated greater comity between States, that is, a greater willingness to recognise and enforce foreign judgments,[43] which would otherwise be problematic in the absence of at least the possibility of the enforcement of the judgment.[44] This, as will be seen, may at least partly explain the continued insistence of enforcement jurisdiction as a prerequisite for the assumption of criminal jurisdiction.

The new test merely required the defendant to have certain 'minimum contacts' with the forum, so much so that the maintenance of suit would not offend 'traditional notions of fair play and substantial justice'.[45] The Court built upon the traditional 'presence' requirement by saying that the term merely symbolised the activities of a corporation in the forum,[46] which in turn meant that whether there were sufficient contacts depended on 'the quality and nature of the activity in relation to the fair and orderly administration of the laws'.[47] The rejection of the traditional criterion of actual presence allowed adjudicative jurisdiction to be imposed upon defendants who, although having substantial

boundaries. The court also listed other bases of jurisdiction, such as the defendant's voluntary appearance or the existence of his or her property within the jurisdiction.

[43] Note that *International Shoe Co*. v. *Washington*, 326 US 310 (1945), was an intrastate dispute, in respect of which the reciprocal enforcement of judgments was and still is much more likely.

[44] In *Hilton* v. *Guyot*, 16 SCt 139, 202f (1895), the US Supreme Court established that comity demands the enforcement and recognition of foreign judgments provided certain prerequisites are satisfied, such as a full and fair trial before the foreign court, the voluntary appearance of the defendant and the existence of reciprocity. See also Jeremy Maltby, 'Juggling Comity and Self-Government: The Enforcement of Foreign Libel Judgments in US Courts' (1994) 94 *Columbia Law Review* 1978.

[45] *International Shoe Co*. v. *Washington*, 326 US 310, 316 (1945); *Shaffer* v. *Heitner*, 433 US 186 (1977) (all assertions of jurisdiction, whether specific or general, had to meet the 'minimum contacts' tests); *McGee* v. *International Life Insurance Co*., 355 US 220, 223 (1957) (the contacts have to create a 'substantial connection' with the forum). The focus in this discussion is only on specific jurisdiction, i.e. where the facts of the dispute arise out of the defendant's contacts with the forum. 'General jurisdiction' concerns circumstances where the defendant's very substantial contacts with the forum justify adjudicative jurisdiction even in relation to a claim which did not arise out of those contacts – a basis rarely if ever of relevance to online activity. ABA, above n. 10, 66.

[46] *International Shoe Co*. v. *Washington*, 326 US 310, 316f (1945). Under English common law, the position is not dissimilar as a company is considered present in a forum if its agent merely carries on business in the forum: *Jabbour* v. *Custodian of Israeli Absentee Property* [1954] 1 WLR 139.

[47] *International Shoe Co*. v. *Washington*, 326 US 310, 319 (1945).

contact with the forum jurisdiction, were formerly beyond the court's reach simply because they were not physically present in the forum at the time of the suit.[48] While it seems that the court abandoned the 'territoriality test', under the motto '[g]eography is not the touchstone of fairness',[49] in fact the territoriality test, albeit a more intangible version, remained:

> increased physical mobility due to automobiles and other modern transportation placed this jurisdictional basis under severe strain, as did disputes over 'virtual' entities such as corporations that have no physical situs . . . As a response to the imminent collapse of jurisdiction based on physical presence, the Supreme Court configured new rules based upon a kind of 'virtual' presence.[50]

Another commentator described the new test as '"neoterritorialist". Jurisdiction continued to be tied to place, but was measured by a more complex relationship with the defendant than simply the location of his body'.[51]

As the new 'minimum contacts' test was broad and rather vague, it was further refined in 1958 in *Hanson* v. *Denckla*, when it was held that an act is required 'by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws'[52] – a test which clearly reflects the no-pain-no-gain notion. So the former test, looking at the presence of the defendant, had now become a test focusing on the objective intentions of the defendant, which requires, unlike the presence test, an evaluation of the defendant's action by the judge hearing the case. Chief Justice Warren in *Hanson* comments: 'the requirements for personal jurisdiction over nonresidents have evolved from the rigid rule . . . to the flexible standard.'[53] But, while both *International Shoe* and *Hanson* 'assumed that a defendant had at some time been physically present in the forum state . . . [and attempted] to overcome the traditional perceived lack of authority to insist a defendant not "caught" within the state return to it to defend a lawsuit',[54] the ever increasing reality was that defendants had never been physically present in the forum despite substantive interaction with it.

[48] But for a few exceptional scenarios, see above n. 42.
[49] *Green* v. *Mason*, 996 F Supp 394, 396 (1998).
[50] Dan L. Burk, 'Jurisdiction in a World Without Borders' (1997) 1 *Virginia Journal of Law and Technology* 1522, paras. 25f.
[51] Stein, above n. 41, 1170. [52] *Hanson* v. *Denckla*, 357 US 235, 253 (1958).
[53] *Ibid*., 251. [54] ABA, above n. 10, 41f.

Thus the 'purposeful availment test' was refined by a holding that it should not be taken too literally.[55] It became sufficient that the defendant in some way through his actions connects or affiliates himself with the forum and thereby invokes the benefits of the forum's law, or targets it.[56] As the jurisdictional breadth became more expansive, the safeguards against excessive jurisdiction became also more elaborate. In *World-Wide Volkswagen Corp.* v. *Woodson*, the Supreme Court held that, even if minimum contacts were present, the court may decline to exercise personal jurisdiction if to do so would not be reasonable, taking into account considerations such as the burden on the defendant, the forum State's interest in adjudicating the disputes, the plaintiff's interest in obtaining convenient and effective relief, and the shared interest of the several States in furthering fundamental substantive social policies.[57] The jurisdictional inquiry was now a two-stage inquiry, with both parts requiring a substantial balancing act by judges. And, to the extent that, for example, the latter test depends on an evaluation of vague notions – such as 'convenient or effective relief', a 'State's interest' or 'fundamental substantive social policies' – the peculiar predicaments and views of the judge hearing the case must come into play.

Commenting on these US developments, Mann already noted in 1964 that a 'perusal of American decisions indicates a tendency to abandon a purely territorial test and to substitute for it a flexible and largely discretionary *notion* based upon the degree of connection'.[58] Yet, this tendency of swapping rigidity and certainty for flexibility and vagueness, fuelled by the desire to keep the no-gain-no-pain rule, had far from reached its climax.

C. *Internet refinements*

Against this legal background, the online revolution occurred. At first, it seemed to make the 'targeting' analysis nonsensical, as every website

[55] *Ibid.*, 43. [56] *Ibid.*, 43ff.

[57] *World-Wide Volkswagen Corp.* v. *Woodson*, 444 US 286 (1980). In England and Australia, similar matters are considered at the *forum non conveniens* stage. *Spiliada Maritime Corp.* v. *Cansulex Ltd (The Spiliada)* [1987] AC 40 (HL). Note that, in *Ocean Sun Line Special Shipping Co. Inc.* v. *Fay* (1988) 165 CLR 197 (HL), 238f, Brennan J rejected a broad *forum non conveniens* test on the ground that it was inimical to the rule of law to repose too wide a discretion in judges to determine the appropriate place of trial. See Brian R. Opeskin, 'The Price of Forum Shopping: A Reply to Professor Juenger' (1994) 16 *Sydney Law Review* 14.

[58] Mann, above n. 15, 46.

may be said to target every State.[59] Thus, some refinement seemed imperative, and this has come in the form of the *Zippo* sliding-scale test. In *Zippo Manufacturing Co.* v. *Zippo Dot Com Inc.*,[60] it was held that the likelihood that personal jurisdiction will be exercised depends on the level of interactivity and the commercial nature of the online exchange of information. The greater the level of interactivity with forum residents and the more the defendant profited or sought to profit from those interactions, the more likely it would be that personal jurisdiction over the foreign defendant will be asserted.

From an outsider's, perhaps European, perspective, these refinements seem like a Chinese whisper, with the final test bearing little, if any, resemblance to what was said at the start; or how does the test of interactivity of a site relate to the tests of 'presence' or 'purposeful availment' or even the latest 'targeting' tests?

> Courts clearly are convinced that the nature of a defendant's web site is relevant to the jurisdictional issue, but a failure to articulate why it is relevant makes it difficult to determine where the jurisdictional line should be drawn in cases that fall between the *Zippo*'s two extremes [i.e. actual and repeated interaction with the forum and a passive site merely posting information].[61]

[59] This explains some early decisions which have applied the targeting approach without making allowance for the fact that every website *prima facie* targets every jurisdiction, e.g. *Inset Systems Inc.* v. *Instruction Set Inc.* 937 F Supp 161 (D Conn. 1996); *Halean Products Inc.* v. *Beso Biological*, 43 USPQ (BNA) 1672 (1997); and *Maritz Inc.* v. *Cybergold Inc.* 947 F Supp 1328 (ED Mo 1996). Some commentators also argue that accessibility of a site should be enough: see e.g. A. Benjamin Spencer, 'Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts' (2006) *University of Illinois Law Review* 71. In the EU context, see e.g. Peter Stone, 'Internet Consumer Contracts and European Private International Law' (2000) 9 *Information and Communication Technology Law* 5.

[60] 952 F Supp 1119, 1124 (WD Pa 1997): 'our review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet . . . At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper . . . At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction . . . The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.'

[61] ABA, above n. 10, 63.

One may even question why the interactive nature of a site should be at all relevant to whether a court does or does not have jurisdiction over a defendant. Assuming its validity, a site which is highly interactive in its design would appear to subject its provider to the personal jurisdiction of every court, and those which are not, of no court at all. But US judges have not defied rationality when finding that the interactivity of a site is relevant to the jurisdictional inquiry. The decisions, but for a few,[62] are sound in themselves. The analysis starts with the premise that the defendant is subject to the jurisdiction of the forum with which he intended – objectively, based on all the facts – to have contact. This means that '[t]he sponsor of a passive website has no way to control which fora she is "connected to" by the site. On the other hand, the site sponsor who does business electronically knows or can take reasonable steps to discover the location of the party with whom she is interacting.'[63]

The sliding-scale test has been attacked by some as not sufficiently anchored in the traditional due-process jurisdiction.[64] That seems an unfair charge, and the argument here is the exact reverse. The *Zippo* test loyally reincarnates the old rules in a new disguise, but this reincarnation is problematic. It makes it more difficult than ever to foresee the outcome. The test creates vast room for disagreement on the precise amount and the nature of the interactivity required to move a site towards either the upper or the lower end of the spectrum. Also, must the interactivity be encouraged or is it enough merely to tolerate it? What is the effect of ring-fencing measures? And does an evaluation of these matters vary depending on the content of the site and the dispute in question? Judges have disagreed – and disagreed strongly.[65] The result

[62] See above n. 59. [63] ABA, above n. 10, 64.

[64] The concept of due process is hardly peculiar to the US; elsewhere it is encapsulated in concepts such as the rule of law and fundamental fairness, protecting those who have done no harm from having to 'travel to a far-off forum to demonstrate that'. Comment, 'No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet' (2003) 116 *Harvard Law Review* 1821, 1824, also 1834f where it is argued that 'the *Zippo* test fails to serve the interests that personal jurisdiction seeks to protect'.

[65] For an early insightful review of the cases and their many inconsistencies, see *Millennium Enterprises Inc.* v. *Millennium Music LP*, 33 F Supp 2d 907 (D Or. 1999). A more recent critique is *Shamsuddin* v. *Vitamin Research Products*, 346 F Supp 2d 804, 809ff (D Md 2004). Compare also e.g. *Euromarket Designs Inc.* v. *Crate & Barrel Ltd*, 96 F Supp 2d 824 (ND Ill. 2000) (one sale which was manufactured by the plaintiff was significant in finding in favour of jurisdiction) and *Stomp* v. *Neat O LLC*, 61 F Supp 2d 1074 (CD Cal. 1999) with *United Cutlery Corp.* v. *NFZ Inc*, WL 22851946 (D Md 2003) and *Millennium Enterprises Inc.* v. *Millennium Music LP*, 33 F Supp 2d 907 (D Or. 1999) (one sale and contacts manufactured by the plaintiff rejected as irrelevant).

is that the 'current hodgepodge of case law is inconsistent, irrational and irreconcilable'.[66] Some have blamed this hodgepodge on the lack of clarity: 'the lack of clarity in lower court opinions in the US simply reflects the lack of clarity in a doctrine that is highly fact specific.'[67] This seems to imply that, provided the doctrine is clarified, everything will be fine. But is it not rather the highly fact-specific nature of the test, its make-up of innumerable variables[68] and its dependence on judges juggling and evaluating innumerable facts that make it likely that different judges will come to different conclusions in respect of similar cases?

Even if it were, for example, firmly accepted that it is the actual interactions with forum residents rather than the site's general interactive capabilities that are relevant,[69] it would only resolve a limited number of inconsistent cases. It certainly would still leave many other variables going into the general pot of judicial decision-making, making it difficult to predict the outcome in a case falling in between the two *Zippo* extremes. While the test is substantively entirely unobjectionable, its application to real factual situations is fraught with difficulties. Its dependence on evaluating innumerable fine factual differences cannot but lead to inconsistent and thus arbitrary decisions – as arbitrary as deciding whether a dark brown egg is a shade more red or yellow or blue.

In short, the desire to provide substantively just outcomes based on the no-gain-no-pain maxim has translated into the need to pursue an increasingly meticulous fact-specific, case-by-case analysis, which threatens certainty and predictability of the law and, with it, the requirement of formal justice. Curiously, the harder States try to accommodate the online phenomenon by refining the law, the more self-defeating the task becomes.

[66] *Millennium Enterprises Inc.* v. *Millennium Music LP*, 33 F Supp 2d 907, 916 (1999), citing Howard B. Stravitz, 'Personal Jurisdiction in Cyberspace: Something More is Required on the Electronic Stream of Commerce' (1998) 49 *SCL Review* 925, 939. For similar sentiments, see also Michael A. Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction' (2001) 16 *Berkeley Technology Law Journal* 1345, 1377. 'Is Zippo's Sliding Scale a Slippery Slope of Uncertainty? A Case for Abolishing Web Site Interactivity As a Conclusive Factor in Assessing Minimum Contacts in Cyberspace' (2001) 34 *John Marshall Law Review* 1051, 1070f (note).

[67] ABA, above n. 10, 57.

[68] A holistic substance approach, taking into account various variables, has frequently been advocated. See e.g. Geist, above n. 66; or Uta Kohl, 'Defamation on the Internet – A Duty Free Zone After All? Macquarie Bank Ltd & Anor v. Berg' (2000) 22 *Sydney Law Review* 119.

[69] *Millennium Enterprises Inc.* v. *Millennium Music LP*, 33 F Supp 2d 907, 922f (D Or. 1999); *GTE New Media Services Inc.* v. *Bellsouth Corp.*, 199 F, 3d 1343, 1350 (D Co. 2000); *Shamsuddin* v. *Vitamin Research Products*, 346 F Supp 2d 804, 809ff (D Md 2004).

The problem associated with the *Zippo* test is not a one-off phenomenon, but pervades potentially the whole spectrum of location-centric tests when applied to transnational online activity (for example, tests seeking to determine *where* a site is 'published' or 'used in commerce'[70]). This is particularly so in the private-law context, where courts often seek to avoid an interpretation of these tests which would lead to worldwide competence. This necessarily requires a nuanced interpretation of the tests which in turn requires a holistic analysis of the site. Of course, courts do not always go along the moderate route, as will become apparent in the next chapter focusing on online defamation.

In the EU, the 'directing test' makes moderation an explicit cornerstone for consumer contracts. Broadly, this test cannot but also require a holistic analysis of websites, weighing innumerable variables, such as the number of transactions with forum residents, the use of a country-specific domain name, the language, the currency of the payments, and any attempts to exclude consumers from certain States as well as offline contacts with the forum – factors which 'are not particularly suitable in creating predictability for the parties'.[71] And yet the Commission, commenting on the newly proposed 'directing test' concerning the applicable law proposals for consumer contracts, seemed unperturbed: 'The sites ... [which attract the protective provisions] are not necessarily interactive sites: a site inviting buyers to fax an order aims to conclude distance contracts. On the other hand, a site which offers information to potential consumers all over the world but refers to a local distributor or agent for the purposes of concluding the actual contract does not aim to conclude distance contracts.'[72] These are safe examples to illustrate a difficult test – a test not difficult to understand, but difficult to

[70] See the discussion in Chapter 2, especially n. 67 and the accompanying text; contrast the non-moderate approach taken in *Cable News Network LP* v. *CN News.com*, 177 F Supp 2d 506 (ED Va 2001), where a website operated by a Chinese resident directed at the Chinese market, which neither sold, nor offered for sale, any goods outside of China, was nonetheless held to be substantially 'used in commerce' in the US by virtue of offering news and information which could be understood by Chinese-speaking US residents.

[71] Oren, above n. 10, 690, where the author validly points out that many of these indicia are often rather ambiguous, particularly if the language used is English and the currency is euros. But see also UK Department of Trade and Industry, *Cross Border Jurisdiction FAQs* (2006), www.dti.gov.uk/consumers/consumer-support/resolving-disputes/Jurisdiction/q-and-a/index.html.

[72] *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations*, COM(2005) 650 final, para. 4.2 (discussion on Art. 5).

implement. The question is what happens to those foreign online providers who, like most online businesses, do not have local distributors in the forum but who nevertheless have regular sales to customers from the forum and whose sales are concluded not by fax, but, much more easily, online. This, of course, is the difficult *Zippo* middle ground.

4. The evolution of jurisdictional rules in public cases

A. Criminal jurisdiction

The rules on criminal jurisdiction may at first seem to have no bearing on online contracts, but of course they do. Online businesses and their contracts clearly are governed not just by contract law. There is a significant body of civil law, such as tort or intellectual property law, which applies to them, and rights arising under these bodies of law may, at most, be excluded only so far as the contracting parties are concerned, but not as concerns strangers. Moreover, criminal and other regulatory law is not something any private individual or company can contract in to or out of. It is the State's prerogative to make, apply and enforce such law as it pleases subject to some restrictions under public international law. In respect of businesses generally, and online businesses in particular, there is a large amount of public law ranging from tax, competition and licensing laws to laws on advertising, health and safety, fraud and the protection of children which is potentially applicable. Online businesses that merely focus on contract law in the transnational context do so at their peril.

A refinement process has also occurred in respect of the jurisdictional rules under public international law which are applicable to criminal and other public law, i.e. those rules in relation to which a State has the prerogative to coerce compliance. This is most apparent in the evolution of the territoriality principle. Given the intended comparison with the above analysis, two matters are worth mentioning first. As noted in Chapter 1, in respect of criminal matters, adjudicative and legislative jurisdiction coincide: 'If the court has jurisdiction, it applies its own law; if the lex fori applies, then the court has jurisdiction.'[73] Thus any inquiry

[73] Michael Akehurst, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145, 179. In domestic law this is, *inter alia*, reflected in the universal principle that the courts of one country will not enforce the penal laws of another country. See generally Matthew Goode, 'The Tortured Tale of Criminal Jurisdiction' (1997) 21 *Melbourne University Law Review* 411, 412.

into the adjudicative jurisdiction of a State court assumes greater significance, as it will also of necessity determine whether the domestic law is applicable to the accused.[74] This, in addition to the criminal nature of the action, makes consistency and predictability even more imperative. This issue of certainty of legal rights and obligations relates to the second point. Given the nature of international law, in particular customary international law, ascertaining clearly defined rules has been notoriously difficult in many areas, not least in relation to jurisdiction:[75]

> Much of the law relating to jurisdiction has developed through the decisions of national courts applying the laws of their own states. Since in many states the courts have to apply national law irrespective of their incompatibility with international law, and since courts naturally tend to see the problems which arise primarily from the point of view of the interests of their own state, the influence of national judicial decisions has contributed to the uncertainty which surrounds many matters of jurisdiction and has made more difficult the development of a coherent body of jurisdictional principles.[76]

[74] This overlap of the two categories has meant that the jurisdictional rules are discussed sometimes as part of prescriptive/legislative jurisdiction (see, for example, Mann, above nn. 15 and 23; Sir Arthur Watts (ed.), *Oppenheim's International Law* (9th edn, London: Longman, 1992); §402 of the US Restatement (Third) of Foreign Relations Law (1986)) and sometimes as part of adjudicative/judicial jurisdiction (see e.g. Akehurst, above n. 73).

[75] In respect of all jurisdictional principles under public international law there is significant disagreement at least in respect of the boundaries cases.

[76] Sir Robert Jennings and Jennings and Watts, above n. 73, vol. 1, 457. On the need for consistency for establishing 'state practice', an element of customary international law, see Donald W. Greig, 'Sources of International Law', in Sam Blay, Ryszard Piotrowicz and Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005), 56f. Some States are likely to be much more influential in shaping certain rules than others: see generally Michael Byers, *Custom, Power and the Power of Rules* (Cambridge: Cambridge University Press, 1999), 40f. Oscar Schlachter, 'New Custom: Power, Opinio Juris and Contrary Practice', in Jerzy Makarczyk (ed.), *Theory of International Law at the Threshold of the 21st Century: Essays in Honour of Krzysztof Skubiszewski* (The Hague: Kluwer, 1996), 531, 537f: 'The more powerful the economy, the greater the presence of its government and nationals in international transactions. Trade, foreign investment, and the technical know-how emanate disproportionately from the advanced economic powers; they carry with them, as a rule, the political views of their respective States, together with social attitudes bearing on international relations. Moreover, for these reasons the affluent States are objects of attention by others. Their views and positions are noticed and usually respected. Their official legal opinions and digests of State practice are available along with international law treatises that influence professional opinion and practical outcomes.'

Bearing these almost conflicting considerations in mind, the following can do no more than demonstrate a trend, rather than clearly reformulated rules. This trend is illustrated mainly by reference to instances of State practice, which in themselves do not necessarily reflect customary international law, but which go far to show that jurisdictional rules under international law have been under similar pressures, and partly driven towards similar refinements, as the rules in respect of private matters. However, there are also some marked differences which are particularly apparent in recent online developments.

B. Pre-Internet refinements

The objective territoriality principle

The territoriality principle, the primary basis of jurisdiction under international law,[77] means that a State has the right to regulate persons, matters and events within its territory.[78] This is reflected in the common law notion that criminal jurisdiction is territorially limited and that all crime is – must be – local.[79] While the territoriality principle seems to provide a fairly clear-cut test, its simplicity is deceptive. It begs the question: what exactly can be said to occur or to be within the territory of a State sufficiently as to give it regulatory power over it? The answer has become more expansive over time so as to 'catch' foreign activity which may have a significant effect on the State's territory as well as generally to avoid situations where transnational crime would go unpunished.[80] Again, this process started long before the Internet in response to greater transnational interactivity.

At international level,[81] the critical decision in respect of the territoriality principle came in 1927 with the *Lotus* case,[82] in which the Permanent Court of International Justice decided that a State may try to punish a person whose foreign acts cause injury within its territory.

[77] Jennings and Watts, above n. 73, 458.

[78] This maxim dates back at least to Ulricus Huber, *De conflictu legum diversarum in diversis imperiis* (1684), reiterated by Justice Story in *The Apollon*, 9 Wheat 362, 370 (1824). See Mann, above n. 15, 24ff.

[79] Goode, above n. 73. Note that common law jurisdictions have always strongly favoured the territorial basis of jurisdiction, unlike civil law jurisdictions, which have traditionally relied more upon the nationality principle.

[80] Goode, above n. 73, 414.

[81] For an excellent overview of how common law courts have manipulated the territoriality principle to accommodate transnational crime, see Goode, above n. 73.

[82] *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No. 10.

Interestingly, the terminology used by Judge Moore is reminiscent of the term of 'symbolic' presence used in *International Shoe*:

> it appears to be now universally admitted that, where a crime is committed in the territorial jurisdiction of one State as the direct result of the act of a person at the time corporeally present in another State, international law, by reason of the principle of *constructive presence* of the offender at the place where his act took effect, does not forbid the prosecution of the offender by the former State, should he come within its territorial jurisdiction.[83]

The fiction of the constructive presence of the offender or the constructive location of the crime within the territory is based upon the injurious effects within the territory of the conduct originating abroad, known as the objective territoriality principle.[84] As noted in Chapter 1, its counterpart, the subjective territoriality principle, permits the State where the crime commenced to assert regulatory control.[85] And these two principles correspond to the country-of-origin and the country-of-destination dichotomy, frequently referred to in the Internet context.[86]

The Permanent Court in *Lotus* redefined the territoriality principle by abandoning the requirement that the offender must be physically in the territory or that the causative act must have occurred there for there to be a valid territorial claim, in favour of a nexus, which merely required the offender's act to affect the territory.[87] In other words, it allowed for a result-oriented jurisdictional claim.[88] This, no doubt, was more attuned to modern conditions which exposed States frequently and substantially to the effects of conduct by absent actors.

[83] *Ibid*., 73 (emphasis added).

[84] This notion has long ago been labelled the 'terminatory theory', as opposed to the 'initiatory theory' in Glanville Williams, 'The Venue and Ambit of the Criminal Law' (1965) 81 *Law Quarterly Review* 518.

[85] *Ibid*.

[86] For example, Hague Conference on Private International Law (Avril D. Haine), *The Impact of the Internet on the Judgments Projects: Thoughts for the Future*, Prel. Doc. No. 17 (2002), 8ff.

[87] Strictly speaking, the *Lotus* case concerns only the constructive location of conduct, rather than the constructive location of the offender, within the territory. The offender has been deemed to be within the territory of a State when, for example, he owns property there, conducts business there or when there is an agent or employee within the territory. See Jennings and Watts, above n. 73, 458f.

[88] Goode, above n. 73, 415f, which is entirely consistent with the evolution of the 'territorial theory' of criminal jurisdiction at common law.

Yet, while the holding appears to adopt a very broad test, the circumstances of the case significantly circumscribed its ambit. First of all, the case concerned the *physical* effects on the territory of conduct originating abroad: the French steamer *Lotus* collided with a Turkish steamer (i.e. Turkish 'territory'), killing eight Turkish sailors and passengers. And, secondly, the effect of the misconduct was a constituent element of the offence: the death of the sailors occurring on Turkish territory was a necessary ingredient or constituent element of the charge of manslaughter under Turkish law. While the Permanent Court seemed at times to use the terms 'effects' and 'constituent element' interchangeably, it also stated that offences 'the authors of [which are] ... at the moment of commission ... in the territory of another State, are nevertheless to be regarded as having been committed in the national territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there'.[89]

It then went on to say that 'the effect is a factor of outstanding importance in offences such as manslaughter, which are punished precisely in consideration of their effect'.[90] So, in *Lotus*, the effect of the conduct was a constituent element of the crime and the court seemed to require that this must be so for there to be territorial jurisdiction.[91] Due to the globalisation of commercial activity, especially after World War II, the requirement for a physical effect came under pressure. As will be seen, the 'constituent element' requirement presents few, if any, hurdles to even the most expansive assertions of competence and simply depends on how the offence is defined by the State.

The 'reasonable' effects doctrine

The next expansion of the territoriality principle came in the form of regulatory claims based on non-physical effects of the foreign activity felt in the State's territory. This occurred in various contexts but the US extraterritorial antitrust enforcement, particularly in the 1970s and early 1980s, caused by far the most controversy. US courts enforced its antitrust law[92] against foreign companies in relation to activities which took place in foreign States on the basis that the effects of those activities were

[89] *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No 10, 23.
[90] *Ibid*., 24. [91] See also the discussion in Mann, above n. 15, 85ff.
[92] Mainly based on the Sherman Antitrust Act (1890). The most influential case, in which the effects doctrine received its classic formulation, is *The Alcoa Case (US* v. *Aluminium Company of America)*, 148 F 2d 416 (1945).

felt in the US. This caused a storm of protest by many States against what was perceived as an excessive extraterritorial exercise of criminal jurisdiction and an attempt to impose US economic policy on other States. This was followed by various blocking and claw-back legislation designed to defeat the outcome of the decisions.[93] Of interest here is that the relevant effects on US territory of the acts originating abroad were certainly not physical effects: they were economic effects, often on US foreign commerce. This acceptance of intangible effects was, if anything, problematic, not – as some have argued[94] – the new doctrine's disregard of the constituent element requirement. That objection is in any event unfounded as the effect is in fact a constituent element of the charge of anti-competitive behaviour.[95] With a little legislative ingenuity, it would be very easy to accommodate some effects within the definition of most crimes. The real problem with the US expansion of the effects doctrine is the intangibility of the effects. If there is no requirement that the effect be physical, the number of States potentially entitled to claim jurisdiction on the basis of the economic effects of foreign activity spirals significantly. In a world where the actions of large companies in one State regularly have an effect across the globe,[96] limitations on the kind of effect required to assert jurisdiction are necessary to prevent multiple claims by all those States affected.

Support for the effects doctrine went hand in hand with support for restrictions on its application. The disagreement has been on the kind of limitations, on whether the effects must be actual or intended or substantial or direct or all of these,[97] and on when these are fulfilled. What all these limitations have in common is their objective, namely, to prevent an unreasonable exercise of jurisdiction or an '*undue* encroachment of a jurisdiction more properly appertaining to ... another State'.[98] The notion of reasonableness is captured in §403(1) of the US Restatement (Third) of Foreign Relations Law (1986), which states that

[93] A.V. Lowe (ed.), *Extraterritorial Jurisdiction – An Annotated Collection of Legal Materials* (Cambridge: Grotius Publications Ltd, 1983), 79ff. E.g. *US* v. *General Electric Co.*, 82 F Supp 753 (1949).

[94] Akehurst, above n. 73, 195, commenting on Mann, above n. 15, 103.

[95] Akehurst, above n. 73, 195f, where he convincingly argues that the economic effects of restrictive business practices are in fact a constituent element of the offence.

[96] For example, Microsoft's worldwide dominance in the field of operating systems.

[97] Akehurst, above n. 73, 199ff. See also §402(1)(c) of US Restatement (Third) of Foreign Relations Law (1986) and Comment d.

[98] *Case Concerning the Barcelona Traction, Light and Power Company Limited (Belgium* v. *Spain) (Judgment)* [1970] ICJ Reports 3, 105 (emphasis added).

'a state may not exercise jurisdiction ... with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable'.

But what is unreasonable? To some extent that must be in the eye of the beholder. And, although §403(2) expressly defines the factors which must be evaluated to decide whether the assumption of jurisdiction would be reasonable, many of these factors are as broad and dependent on value judgments as the term they seek to define: the extent to which the activity has a *substantial, direct or foreseeable effect* upon the territory, the *character* of the activity and the degree to which the *desirability* of regulation is *generally accepted*, the existence of *justified expectations*, the *importance* of regulating the activity and the *consistency* with *traditions of the international system* and the *interests of other States* in regulating the activity, and finally the *likelihood* of conflicting regulations.[99] Löwenfeld, who wrote these provisions, noted that 'our aim is reasonableness, not certainty'.[100] As an attempt to provide for a fair and balanced division of regulatory power this approach is praiseworthy; on substantive justice grounds, it is entirely correct. There has been high-profile academic, governmental and judicial support for such a flexible, holistic analysis and balancing act.[101] Mann captures this holistic approach when he notes that '[p]erhaps public international lawyers should now discard the question whether the nature of territorial jurisdiction allows facts to be made subject to a State's legislation. Rather they should ask whether the legally relevant facts are such that they "*belong*" to this or that jurisdiction.'[102]

[99] This echoes the balancing test advocated by Judge Choy in *Timberlane Lumber Co.* v. *Bank of America* 549 F 2d 597, 611–12 (1976). For a discussion of a not dissimilar list, see Goode, above n. 73, 443f.

[100] Andreas F. Lowenfeld, 'Public Law in the International Arena: Conflict of Laws, International Law and Some Suggestions for Their Interaction' (1979) 163 *Recueil des Cours* 311, 329. See also S. Dodge, 'Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism' (1998) 39 *Harvard International Law Journal* 101, 137.

[101] A similarly holistic approach was taken in the *Nottebohm Case (Liechtenstein* v. *Guatemala)* [1955] ICJ Reports 4, where the International Court of Justice applied the principle of a 'genuine link' in the nationality context. See also Lowe, above n. 93, 94 (Australian support of the balancing-of-interest test, provided it is not applied by the judiciary), 108f (Canadian approval of a balancing of interests approach), 207ff (European Community commenting on the balancing-of-interests approach, arguing that it should also be applied at the rule-making stage).

[102] Mann, above n. 15, 45.

And, after initial hesitation as to whether the territorial principle in its simplicity is perhaps after all 'preferable to a more elaborate and refined, but also more hazardous, version',[103] he goes on to pre-empt critics of the flexible test:

> It may be said that the test . . . would substitute vagueness for certainty. This would be formidable criticism if the principles of jurisdiction in fact were at present defined with certainty. But the simplicity of Huber-Storyan teaching is deceptive. The question, for instance, where a crime or tort is committed is subject to so much doubt that no certain answer can be suggested in any but the clearest cases; nor has the territorial test led to much certainty in the field of trade practices or taxation.[104]

But the fact remains that a more elaborate and refined version of the territoriality principle is a yet more hazardous and uncertain basis of jurisdiction (albeit rationally more satisfactory) than its cruder predecessor. This increased uncertainty is illustrated by the protests against the US antitrust approach, which was on the whole not based on the substantive unfairness of the effects doctrine but on what the US regarded as falling within it. Some States expressly rejected the effects doctrine because of its inherent uncertainty.[105] In terms of substantive justice, it is entirely unobjectionable; in terms of formal justice it fails.

Return to a 'crude' effects doctrine

There has been a backlash against this flexible approach. For example, in the case of *Hartford Fire Insurance Co.* v. *California*, where the court held that international comity, or the test of reasonableness and the notion of 'comparative interest balancing', should only come into play if there is a 'true conflict between domestic and foreign law'.[106] The judgment is generally viewed[107] as the return to a more expansive, cruder effects doctrine and has been applauded for its greater legal certainty:

> The task of identifying, explaining, and weighing the comparative regulatory interests of different nations in any given international

[103] *Ibid.*, 43. [104] *Ibid.*, 50.

[105] For example, for the United Kingdom, see Submission of the British Attorney General to the House of Lords in *In re Westinghouse Electric Corporation Uranium Contracts Litigation* in Lowe, above n. 93, 170. But cf. Akehurst, above n. 73, 208 (on the UK attitude to the effects doctrine).

[106] *Hartford Fire Insurance Co.* v. *California*, 509 US 764, 798 (1993).

[107] E.g. Dodge, above n. 100; also Hannah L. Buxbaum, 'The Private Attorney General in a Global Age: Public Interests in Private International Antitrust Litigation' (2001) 26 *Yale Journal of International Law* 219.

> transaction is virtually impossible for courts and private litigants ... [T]he assumption that ... [these] rules enhance the predictability of international transactions by identifying a single national regulatory regime ... seems completely belied by the ex post and inexact nature of the various interest balancing rules for selecting a single applicable law. It typically would be far more predictable and less burdensome for an international transaction to comply with the regulatory regimes of multiple nations so long as that prospect is known beforehand and accounted for when the transaction is structured.[108]

The US has not been alone in endorsing a more expansive effects doctrine in response to transnational crime. For example, under s.10C of the Crimes Act 1900 (NSW) a person is deemed to have committed an offence in New South Wales if 'the offence is committed wholly outside the State, but the offence has an effect in the State'.[109] This approach sits comfortably with the view of the Australian High Court which has expressed a clear willingness to reconsider jurisdictional rules in view of increasing transnational crime: 'Trans-jurisdictional commerce and intercourse ... is now accomplished with such speed and facility, that for many purposes jurisdictional boundaries are irrelevant. They remain relevant for purposes of criminal law, but there is every reason to apply the law in a manner which accommodates the reality.'[110]

According to the majority, modern reality should be accommodated by not insisting on too taxing a link or nexus between the activity and Australia: 'The requirement of nexus should be liberally applied. A real connection with the jurisdiction will suffice.'[111] Here the real nexus was

[108] Philip J. McConnaughay, 'Reviving the "Public Law Taboo" in International Conflict of Laws' (1999) 35 *Stanford Journal of International Law* 255, 257.

[109] This section, introduced by the Crimes Legislation Amendment Act 2000, was intended to overcome the effect of *R* v. *Catanzariti* (1995) 65 SASR 201, which concerned a conspiracy in South Australia to cultivate cannabis in the Northern Territory. The judge held that the accused had not committed an offence in South Australia as the object of the conspiracy was to breach a foreign criminal law, that is, the law of the Northern Territory.

[110] *R* v. *Lipohar* (1999) 168 ALR 8, para. 37 (Gleeson J); cf. *ibid*., paras. 186ff, where Kirby J agrees with the majority that the elements of the crime occurred outside the State, but disagreed with them that, despite this, the South Australian court could assert criminal jurisdiction.

[111] *R* v. *Lipohar* (1999) 168 ALR 8, para. 123 (Gaudran, Gummow and Hayne JJ). Under public international law, the nationality of the victim is a nexus accommodated by the passive personality principle, which does not enjoy universal acceptance. Akehurst, above n. 73, 163. But, as the above case was an intra-state case, the limitations under public international law were irrelevant.

simply the nationality of the victim company, which Callinan J defends on the basis of the conceptual difficulties associated with the traditional territorial test in the context of conspiracy. This broad test would provide flexibility and 'is, as a test, no less exact than many which common law courts are regularly called upon to apply'.[112]

The problem with this expansive test, as with the expansive effects test, is not its uncertainty; those engaged in transnational conduct can predict that most links with a State will expose them to its laws. Rather, the problem is its breadth and thus the regulatory burden it imposes on transnational actors. The question addressed now is what impact, if any, the Internet has had on the evolution of the territoriality principle and its interpretation.

C. Internet developments

Although it is too early to assess the full impact of the Internet on jurisdictional doctrines, it is already clear that States strongly endorse a country-of-destination approach. Furthermore, States tend to find in favour of their regulatory right on the basis that a constituent element of the offence has occurred on their territory (i.e. objective territoriality principle) without considering whether the effects of the site on their territory were anything but minimal. Mere accessibility of the site tends to be sufficient. Whether or not the assertion of competence would be reasonable does not enter the inquiry. The prominence of an effects test generally is not surprising given that it seems tailor-made for the online environment where the effects of foreign online conduct are often the only nexus upon which a State can rely to assert a regulatory right over activities which infiltrate its territory. What is surprising is that the moderate effects doctrine, imposing a standard of reasonableness, comparable to the approach taken in private matters, has not – bar few exceptions – been endorsed by States. The particular criminal context within which the issue of criminal jurisdiction has arisen has varied from State to State consistent with their varying regulatory priorities, but the approaches are in result often indistinguishable. Notably, too, most of the cases mentioned below involve commercial actors and their commercial activities on foreign shores.

In the US, online gambling, and in particular foreign online gambling operators (discussed in depth in Chapter 5), has been the *enfant terrible* of online activity, or at least one of them. For example, in *People* v. *World*

[112] *R* v. *Lipohar* (1999) 168 ALR 8, para. 269 (Callinan J).

Interactive Gaming Corp.,[113] a New York court held that it could enjoin an Antiguan corporation, legally licensed to operate a casino in Antigua, and its Delaware parent company from offering gambling opportunities to Internet users in the State of New York. The court justified personal jurisdiction *inter alia* on the basis that the gambling website was targeted at the US and was known to attract thousands of New Yorkers, and subject-matter jurisdiction on the basis that the gambling had occurred in New York by New Yorkers entering and transmitting the bets.[114] A constituent element of the offence had occurred in New York. This was an easy case as the foreign defendants and their business activities had other substantial connections with New York. Even on the application of the 'reasonable' effects doctrine, competence could easily be justified. The court noted that '[a] computer server cannot be permitted to function as a shield against liability, *particularly* in this case where respondents *actively targeted* New York as the location where they conducted *many* of their allegedly illegal activities'.[115] The question which remains open is whether a computer server may be a shield against liability where the online activity does not actively target the State, but may nevertheless have some minor effect on the State. The answer is likely to be 'no'.

In Australia, the question of criminal jurisdiction has, for example, come up in respect of online securities dealings. The Australian Securities and Investments Commission, in its policy statements on 'Offers of Securities on the Internet' and 'Electronic Prospectuses', states that it does not intend to regulate foreign online offers, invitations or advertisements of securities if (1) they are not targeted at persons in Australia, or contain a meaningful disclaimer; (2) they have no or little impact on the Australian market; *and* (3) there is no misconduct.[116] At first sight, this test seems rather reasonable and restrained, similar to the US case above. It considers whether the effects of the foreign activity on Australia were intended and substantial (i.e. 'reasonable' effects

[113] 714 NYS 2d 844 (1999).

[114] *Ibid.*, 849, 850 (1999). In the US, unusually, even in criminal cases a distinction is made between adjudicative and legislative jurisdiction.

[115] *People* v. *World Interactive Gaming Corp.*, 714 NYS 2d 844, 850 (1999) (emphasis added).

[116] Australian Securities and Investments Commission, *Offers of Securities on the Internet*, Policy Statement 141 (10 February 1999, reissued 2 March 2000), PS 141.5, 141.14, 141.16; and *Electronic Prospectuses*, Policy Statement 107 (18 September 1996, reissued 10 February 2000), PS 107.102.

doctrine). Yet, a careful reading of the test reveals that jurisdiction may be asserted simply on the basis of misconduct. And that misconduct may of course be established in respect of *any* site that is merely accessible in Australia. The commentary expressly states that an offer of securities is made in Australia and thus subject to Australian securities regulation 'if it is received in Australia. This means that the Law may apply to offer or invitation of securities on an Internet site *accessible* from Australia irrespective of where the offeror is located.'[117]

In the UK, as in many other States, the easy online accessibility of pornography to children has been a cause for concern. In *R* v. *Perrin*,[118] Perrin, a French national resident in England, was convicted for the offence of publishing an obscene article contrary to the Obscene Publications Act 1959 in relation to a freely accessible preview site for a pornography subscription website.[119] Perrin appealed *inter alia* on the basis that the site had been uploaded on a server abroad,[120] and thus, he argued, applying UK criminal law to the site would be inconsistent with his right to freedom of expression. The Court of Appeal rejected that argument. If the country of origin of the material was the only country entitled to regulate it, it would undermine local laws and encourage forum shopping by online publishers.[121] Noteworthy here is that there was no evidence that anyone in the UK had actually accessed the material apart from an officer of the Metropolitan Police: it was the

[117] Australian Securities and Investments Commission, *Offers of Securities on the Internet*, Policy Statement 141 (10 February 1999, reissued 2 March 2000), PS 141.10 (emphasis added).

[118] [2002] EWCA Crim 747. Perrin's application to the European Court of Human Rights, that with his conviction and sentence the UK had breached his right to freedom of expression, was rejected: *Perrin* v. *UK* (ECHR 18 October 2005, No. 5446/03).

[119] Perrin was convicted and sentenced to two-and-a-half years' imprisonment. Section 2(1) of the Obscene Publication Act 1959 provides: 'any person who, whether for gain or not, publishes an obscene article or who has an obscene article for publication for gain . . . shall be liable on summary conviction [or on conviction on indictment] to a fine . . . or to imprisonment . . .'. For a similar provision in Australia, see s.578C of the Crimes Act 1900 (NSW); discussed in Gareth Griffith, *Censorship in Australia: Regulating the Internet and other Recent Developments*, Briefing Paper (April 2002).

[120] It appears that he admitted that he was a director and/or majority shareholder of one or more US companies involved in operating the website from the US. Online updates to Graham J. H. Smith, *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002), para. 12-067, www.smlawpub.co.uk/online/intereg/apr02.cfm.

[121] For a discussion of the case, see Michael Hirst, 'Cyberobscenity and the Ambit of Criminal Law' (2002) 13(2) *Computers and Law* 25; Uta Kohl, 'Who Has the Right to Govern Online Activity? A Criminal and Civil Point of View' (2004) 18 *International Review of Law, Computers and Technology* 218.

mere accessibility of the site which led to the conclusion that there was 'publication' on British soil.[122] The effects on British territory might have been absolutely minimal but that mattered not.

France and Germany on the other hand have been concerned by the easy online accessibility of Nazi memorabilia, contrary to the criminal laws of both States. In *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France*, discussed further in Chapter 6, the Paris District Court held that Yahoo! Inc., incorporated in the US with its principal place of business in California, must make it impossible for surfers from French territory to access Nazi memorabilia via its site – a site which was primarily aimed at a US audience.[123] Although the case was on its face a private matter (arising under the New Code of Civil Procedure which allows a French court to issue an injunction to stop a manifestly illegal disturbance), in substance it was based on a breach of French criminal law and arguably the eventual court order was a criminal penalty and not a private remedy.[124] Thus the limits of criminal jurisdiction under public international law should have informed the judgment. The court certainly never referred to those limits and simply asserted regulatory competence on the basis that, by 'permitting the visualisation in France of these objects and eventual participation of a surfer established in France in

[122] The Court acknowledged the possibly minimal effect of the site in Britain, when it said that in this case there was no need to confuse the jury 'by a direction that the effect of the article must be such as to tend to deprave and corrupt a significant proportion, or more than a negligible number of likely viewers'. *R* v. *Perrin* [2002] EWCA Crim 747, para. 30.

[123] *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000), affirmed in *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000), www.foruminternet.org/actualites/lire.phtml?id=273.

[124] The actual illegality consisted of a violation of the French Criminal Code, which makes the distribution of the Nazi material illegal. This, in addition to the onerous injunction as well as penalty imposed (Yahoo! Inc. was ordered to comply with the injunction within three months, after which time it would incur a penalty of 100,000 francs for every day of delay), creates room for arguing that the judgment was in fact a penal judgment. This was argued by Yahoo! Inc. in its complaint (filed on 21 December 2000 in the US District Court, Northern District of California; No. C00-21275) in which it sought declaratory relief that the French orders were neither recognisable nor enforceable in the United States. Personal jurisdiction held to be established in *Yahoo! Inc.* v. *LICRA and UEJF*, 145 F Supp 2d 1168 (ND Cal. 2001). In *Yahoo! Inc.* v. *LICRA and UEJF*, 169 F Supp 2d 1181, 1192f (ND Cal. 2001)), the court seems to assume that the judgment was not penal but still not enforceable as it was inconsistent with the First Amendment to the US Constitution; reversed on appeal in *Yahoo! Inc.* v. *LICRA* and *UEJF*, 433 F 3d 1199 (9th Cir. 2006). The judgment's criminal character also seems to be assumed in the discussion in ABA, above n. 38, 83.

such an exposition/sale, Yahoo! Inc. ... committed a wrong on the territory of France'.[125] Justice Gomez seems to have based jurisdiction on the fact that a constituent element of the offence took place on French territory: the exhibition of the offending material. He noted: 'the harm is suffered in France, our jurisdiction is therefore competent.'[126] Again, the mere accessibility (without any evidence of intentional and substantial directing of the site to France) triggered French law. Noteworthy though, in the later judgment, concerning the feasibility of blocking French users, the court stressed that yahoo.com had aimed 'at a French audience since it responds to a connection to its auction site from a computer located in France by dispatching advertising banners in French'.[127] But did the site in fact have a substantial effect on French territory so as to make an assertion of regulatory competence reasonable? In respect of a potential criminal prosecution of Yahoo! Inc. and its CEO, Timothy Koogle, arising out of the same facts, the Paris court took a similarly robust approach to jurisdiction:

> Concerning media, advertising is one of the constitutive elements and even the essential characteristic of the offences created ... by the [relevant] law ... For the present case, providing at the public's disposal an online auction of Nazi objects, which can be seen and received on French territory and to which the Internet users can gain access because of the simple existence of a computing link 'search' inviting him to search, characterises the advertising element necessary to constitute the offence of apology of war crimes and this is so, whether the Internet user was specifically targeted by the owner of the website.[128]

Once again, the court took a pure constituent-element approach, and the critical fact establishing that element was the mere accessibility of the site on the State's territory.

A marginally less extreme conclusion (given perhaps slightly more favourable facts) was reached by the German High Court when it decided that foreigners may be prosecuted in respect of their online activities, even if those activities originate abroad.[129] The case concerned

[125] Tribunal de Grande Instance de Paris, 22 May 2000. [126] *Ibid*.

[127] Tribunal de Grande Instance de Paris, 20 November 2000.

[128] *R* v. *Timothy K and Yahoo Inc*. (Tribunal de Grande Instance de Paris, 26 February 2002, No. 0104305259), 10, www.foruminternet.org/actualites/lire.phtml?id=273.

[129] *Töben* (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624; discussed in Yulia A. Timofeeva, 'Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis' (2005) 20 *Connecticut Journal of International Law* 199, 206f.

the Australian citizen, German-born Frederick Töben, who had published in Australia anti-semitic material on his homepage entitled 'Adelaide Institute'.[130] In his publications, mass murder committed by Germans during World War II is denied and presented as a Jewish myth and backed by alleged research and scientific proof, in violation of German criminal law. The court asserted jurisdiction on the basis of the objective territoriality principle, arguing that a constituent element of the crime had occurred in Germany, consisting in the real capability of the online material to disturb the public peace in Germany.[131] The German court seemed to make an attempt to show why Germany may have a stronger claim than other States to apply its criminal laws to Töben's publication. It argued that, given Germany's history, there is objectively a special link between the material in question and the German territory, which justifies the assertion of jurisdiction.[132] It also reasoned, given the focus of the site on Germans and German history, that German surfers, in particular, were part of the intended and actual addressees of the site.[133] Although these arguments have some persuasive power, the holding does not sit easily with the fact that the topic of the site is of universal interest and that the online publication was in English. Also, there was in fact no evidence that, apart from the investigating police officers, anyone in Germany had actually accessed the site.[134] Indeed, it has even been questioned whether this Australian site, set up by a self-appointed historian from a dubious institute, was at all capable of having the effect in Germany required for the commission of the offence in question.[135] Was it capable of undermining the general population's or the Jewish community's trust in the public order? Given that the answer to this question can only be negative, it is tempting to see the case as designed to be a show case for demonstrating the unacceptability, offline or online, of radical right-wing views.[136]

[130] Töben had already been ordered to remove the relevant material on the basis that it was contrary to the Racial Discrimination Act 1975 (Cth): *Jeremy Jones and Member of the Committee of Management of the Executive Council of Australian Jewry* v. *Frederick Töben* (Australian Human Rights and Equal Opportunities Commission, 5 October 2000), affirmed in *Jones* v. *Töben* [2002] FCA 1150.

[131] *Töben* (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624, 627.

[132] *Ibid*., 628. [133] *Ibid*., 626f. [134] *Ibid*., 625.

[135] Irini E. Vassilaki, 'Anmerkung' (2001) 4 *Computer und Recht* 262, 265.

[136] Ellen S. Podgor, 'International Computer Fraud: A Paradigm for Limiting National Jurisdiction' (2002) 35 *University of California Davis Law Review* 267, where the author argues that a reasonableness test should temper jurisdictional claims.

The above cases, slight variations apart, illustrate the proposition that States on the whole need very little factual basis to find in favour of a nexus justifying, the imposition of their criminal law on foreign online activities. Frequently, the mere accessibility of a site in the State suffices to establish that an element of the crime has occurred on the territory. In many ways, this approach suffers the exactly opposite problems and advantages of the approach taken in private matters: formal justice presents few concerns, as it should be clear to online actors that a mere online presence is likely to expose them to foreign criminal laws. This is a very predictable and clear position, but is it substantively fair?

Given that the transnationality of the Internet essentially presents the same kind of challenge for both criminal and civil regulation, it is surprising that the legal responses vary. Why have the doctrinal developments in respect of criminal jurisdiction not gone down a path of refinement comparable to that taken in private matters? The common denominators of the above criminal decisions may help to throw some light onto the underlying reasons.

D. The common denominators

The possibility of concurrent jurisdiction

In most of the above judicial authorities, what is conspicuous by its absence is any reference to the laws of other States and the potential for conflicting regulation or overregulation. Certainly, there is nothing even resembling the balancing approach advocated in the antitrust context and the US Restatement (Third) of Foreign Relations Law (1986). The closest the decisions come to acknowledging the existence of foreign law is by discounting it as irrelevant. Even in *People* v. *World Interactive Gaming Corp.*, the court actually stated that '[i]t is irrelevant that Internet gambling is legal in Antigua'.[137] The question is why there has been this apparent indifference to the laws of other States, with courts treating the cases as almost purely domestic matters.

The answer may be found in the online case which did spark some real controversy, namely, the CompuServe incident in Germany in 1995

[137] *People* v. *World Interactive Gaming Corp.*, 714 NYS 2d 844, 850 (1999). See also *US* v. *American Sports Ltd*, 286 F 3d 641 (2002) where it was held irrelevant whether gambling was legal in Britain; and *R* v. *Timothy K and Yahoo Inc.* (Tribunal de Grande Instance de Paris, 26 February 2002, No. 0104305259), 10, where the court stated that it is irrelevant whether the publication is criminal in the country of origin.

when 'CompuServe blocked access to 200 chat groups for fear of prosecution under Bavaria's obscenity laws. Because CompuServe did not have the technology to ban the groups only to its 220,000 customers in Germany, it had to ban the groups worldwide, suspending access to four million subscribers in 147 countries.'[138] The outrage was based on the fact that here Germany indirectly imposed its moral standards across the globe. And this is precisely why more recent decisions have been more acceptable. In none of them did the courts require an end to the provision of gambling services or Nazi items or propaganda everywhere, but just on their territory. And the courts decided this, and could decide this, because content providers are able to territorially restrict their sites. Indeed, the French court went to some trouble to verify the practical feasibility of its order.[139] And, although the New York court rejected the respondent's argument that it unknowingly accepted bets from New York residents, it seems likely that it would have accepted it if the casino's software, intended to filter out New York residents, had been less prone to circumvention by New York gamblers.[140] Thus, the judgment is in line with the French judgment in requiring the providers of certain content to make their sites territorially sensitive. Provided that each State only claims jurisdiction over a site as far as it affects the State's territory and no further, conflicting claims cannot arise, and therefore there is no need to consider the laws of other States. This in turn makes the holding of the US District Court in *Yahoo! Inc.* v. *LICRA*, that the French order was inconsistent with the First Amendment to the US Constitution and thus not enforceable in the US, highly questionable,

[138] John F. McGuire, 'When Speech is Heard Around the World: Internet Content Regulation in the United States and Germany' (1999) 74 *New York University Law Review* 750, 769 (footnotes omitted). The CEO of CompuServe was acquitted on appeal of the charge of facilitating the distribution of child pornography in Germany by allowing access to a US news server: *R* v. *Felix Somm, CEO of CompuServe GmbH* (AG München I, 17 November 1999–20 Ns 465 Js 173158/95), www.computerundrecht.de/1672.html. See also Oliver Zander, 'Recent Developments in German Internet Law' (October/November 2000) *Computer and Law* 36, 36.

[139] Tribunal de Grande Instance de Paris, 11 August 2000, where the Paris court ordered the setting up of a three-member panel of experts to comment on the feasibility of ordering Yahoo! Inc. to prevent French surfers from accessing neo-Nazi material. The finding of the panel formed the basis of the November judgment. Note, geo-location technology has come quite a long way since then: Dan Jerker B. Svantesson, 'Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet' (2004) 23 *John Marshall Journal of Computer and Informational Law* 101.

[140] *People* v. *World Interactive Gaming Corp.*, 714 NYS 2d 844, 861 (1999).

given that the French order never purported to affect what Yahoo! Inc. would release to its US customers.[141] But more on that in Chapter 6.

In short, the development of technical means of territorially restricting sites facilitates the possibility of concurrent jurisdiction, i.e. States can apply their laws to online conduct without unduly encroaching upon the jurisdiction of other States. States have not protested against recent assumptions of jurisdiction because, unlike the German CompuServe case, they do not preclude concurrent regulation. For example, when the New York court asserted that the gambling activity was legal in Antigua, it implied that Antiguan law was in fact also applicable to the activity, and that the company should be free to enjoy that legality in Antigua. The problem with concurrent jurisdiction is that it either discourages most online businesses from taking advantage of the international nature of the Internet (i.e. the very thing which makes it so revolutionary) or it imposes an extremely high regulatory burden on those businesses which are not discouraged – potentially the burden to comply with the laws of every single State.

But one may object that concern about overregulation, although often voiced, is perhaps exaggerated: States have not taken action in respect of foreign online activity as readily as might have been expected. Given the vast amount of online activity, the number of cases in which States have actually sought to assume jurisdiction over foreign online activities is astonishingly small. This seems paradoxical, particularly in view of the wide breadth of competence asserted by States, as noted above. The answer lies in another common denominator.

Insistence on enforcement jurisdiction

In all of the above cases, the regulating State had some actual power over the foreign provider at least to the extent of ensuring that the accused would answer the charges. For example, in *People* v. *World Interactive Gaming Corp.*, the Antiguan company was a wholly owned and controlled subsidiary of World Interactive Gaming Corp., a Delaware company, which in turn had corporate offices in the forum, i.e. New York. In the case of *US* v. *American Sports Ltd*, the US successfully pursued an online gambling business originating from the UK, given that one of the

[141] *Yahoo! Inc.* v. *LICRA*, 169 F Supp 2d 1181, 1192f, 1194 (ND Cal. 2001): 'In light of the Court's conclusion that enforcement of the French order by a United States court would be inconsistent with the First Amendment, the factual question of whether Yahoo! possesses the technology to comply with the order is immaterial.'

defendant companies was a New Jersey corporation and that the businesses had US bank accounts.[142] In the French Yahoo case, Yahoo! Inc., a Delaware company, had a French subsidiary, Yahoo France.[143] However, the Paris court did not allow for the orders against Yahoo! Inc. to be enforced against its French subsidiary, and it even acknowledged the enforcement difficulties arising out of this.[144] In *Perrin*, the accused was a resident of the UK. And, finally, the German judgment arose out of a case in which, following his arrest in Germany, Töben had been sentenced to ten months' imprisonment for distributing revisionist leaflets in Germany.[145] Thus, in the decided cases, the regulatory right asserted was backed by might. The insistence by States on the existence of enforcement power in the criminal context[146] is based on a fear of wasted public resources if a conviction cannot be enforced[147] and, to a lesser extent, on a concern for fairness towards the accused.

[142] *US* v. American Sports Ltd, 286 F 3d 641 (2002), which concerned the US government's *in rem* forfeiture action against the funds, i.e. proceeds from the illegal gambling activities, in the US bank account.

[143] Although the Paris court (like the courts in the other examples) never expressly acknowledged that this was the trigger for its assumption of jurisdiction, it would explain why other foreign online culprits have not been sued or prosecuted. See Lyombe Eko, 'Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation' (2001) 6 *Communication Law and Policy* 445, 472f: 'Though other online auction sites, such as eBay, display and auction memorabilia from Hitler's Third Reich, Yahoo! was sued because it had a French subsidiary.'

[144] Tribunal de Grande Instance de Paris, 20 November 2000.

[145] *Töben* (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624, 625; although it seems that at the time of the ruling Töben had returned to Australia. See 'Holocaust Denier Not Impressed by Ruling', *Frankfurter Allgemeine Zeitung* (English edn, 13 December 2000), www.faz.com.

[146] States will not generally enter a default judgment against an absent accused. *Lipohar* v. *R* (1999) 168 ALR 8, 26. *R* v. *Manning* [1999] 2 WLR 430, 444: 'The English courts had jurisdiction subject to two conditions: that the defendant was physically present before the court (a matter that cannot be affected by construction of the statute) and that he had completed the crime, as defined, within England and Wales.' See generally Ivan Shearer, 'Jurisdiction', in Sam Blay, Ryszard Piotrowicz and Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005), 154.

[147] No State will enforce the public law/judgments of another State. But note that, in the context of private disputes, under Art. 7 of the Rome Convention on the Law Applicable to Contractual Obligations (1980), a State may give effect to the 'mandatory rules' of another State. These mandatory rules are not strictly speaking 'public law' as it is private litigants who routinely enforce them, rather than the State. For further discussion on the nature of public law/judgments, see Chapter 6. On the development of 'mandatory rules', see Max Planck Institute for Foreign Private and Private

The frequent lack of enforcement jurisdiction in respect of online conduct has no doubt played a significant role in keeping a lid on the number of cases where States would otherwise have asserted jurisdiction. This may also explain why States, on those fairly rare occasions when in possession of enforcement power, have not been too concerned about the limits of their legislative/adjudicative jurisdiction under public international law. It is telling that, of all the instances of State practice mentioned above, the only reference to the requirements of international law is made in the German judgment.[148] This combination of very expansive regulatory claims in principle coupled with the very few opportunities to enforce them seems to make an unhappy marriage. Perhaps this means that territorially focused criminal law is also moving towards a tipping point, albeit not because it is too refined but because it is fair neither on individuals nor on States.

The fact that the existence of enforcement jurisdiction tends to be perceived as a prerequisite for excising adjudicative/legislative jurisdiction in respect of transnational criminal activity means that the subjective territoriality principle, i.e. the country-of-origin approach, is far more user-friendly for States. There, jurisdiction is based on the fact that the activity originated from the State's territory, and so it invariably goes hand in hand with enforcement jurisdiction: the person responsible for the acts tends to be on the State's territory. The subjective territoriality principle underlay the Canadian Internet Holocaust denial case (again arguably a private rather than a criminal case[149]). Ernst Zündel was alleged to have violated s.13 of the Canadian Human Rights Act 1985 by publishing his views, through his US employee, on a website known as the 'Zündelsite' located in California. Jurisdiction was based not on the effects, one way or another, of the US site on Canadian territory, but rather on the control Zündel asserted over the content of the site and

International Law, *Comments on the European Commission's Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument* (2003), 56ff, http://ec.europa.eu/justice home/news/consulting_public/rome_i/news_summary_rome1_en.htm.

[148] *Töben* (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624, 628.

[149] The claim was brought by the private complainant, Sabina Citron, parallel to the complaint filed by the Mayor's Committee on community and Race Relations in respect of discriminatory practices under s.13(1) of the Canadian Human Rights Act which, when proven 'on a preponderance of evidence' (a civil standard of proof), entitles the complainant to 'corrective' remedies rather than giving rise to criminal penalties: *Citron* v. *Zündel* (No. 4) (2002) 41 CHRR D/274, para. 38, paras. 295ff, www.chrt-tcdp.gc.ca.

thus by reference to Zündel's relationship to the webmaster, Dr Ingrid Rimland.[150] In other words, it was based on the fact that Zündel in Canada caused the offending site to be published. Similarly, in the clearly penal case of *People* v. *World Interactive Gaming Corp.*, the allegations against both defendants were at least partly founded upon the fact that the 'activity was transmitted from New York. Contrary to the . . . allegation of an Antiguan management company managing GCC, the evidence also indicates that the individuals who gave the computer commands operated from WIGC's New York office'.[151] In short, the State from which the activity in substance originated was New York.

Yet, just because the country-of-origin principle does not suffer from the same enforcement difficulties as the country-of-destination principle,[152] does not mean, as the cases above show, that States are prepared to surrender jurisdiction based on the latter principle. This is even more the case in respect of certain types of crimes, which brings us to the third common denominator of the above decisions.

Lack of international consensus: moral and cultural values

All the above cases were concerned with controversial activities even in States which tolerate them, such as unlicensed gambling, the free availability of pornography or the publication of Nazi propaganda. Yet, though controversial, they concern activities in respect of which there is no international consensus as to whether and, if so, how to regulate them. For example, while hate speech is tolerated in the US[153] and a

[150] *Zündel* v. *Canada* (1999) 175 DLR (4th) 512, paras. 62–6. For an overview of the case history and the final ruling by the Canadian Human Rights Tribunal, see *Citron* v. *Zündel* (No. 4) (2002) 41 CHRR D/274. In 2005, on his return to his native Germany (being deported from the US and then Canada), Zündel was charged with the offences of inciting racial hatred and defaming the memory of the dead, based on the publications of his website.

[151] *People* v. *World Interactive Gaming Corp.*, 714 NYS 2d 844, 850f (1999).

[152] The Tribunal in *Citron* v. *Zündel* (No. 4) (2002) 41 CHRR D/274, paras. 295–302, commented on the likely enforceability of the order and responded to the contention that mirror sites can easily defeat the order by noting that the order not only serves the purposes of prevention and elimination of discriminatory practices but also has a significant symbolic value. Approved in *Jones* v. *Töben (including explanatory memorandum)* [2002] FCA 1150, para. 111.

[153] *Brandenburg* v. *Ohio*, 395 US 444 (1969). The fact that the advocacy of racist theories is protected under the First Amendment to the US Constitution does not mean that the ideas themselves received judicial approval but rather that it is perceived that market forces can deal with them more effectively than suppression of such undesirable ideas.

criminal offence in France and Germany,[154] Canada and Australia have gone the middle way and created a private cause of action in respect of it.[155] The approaches to the regulation of these activities reflect States' national moral values and cultural identities.[156] So, in as much as the criminalisation of hate speech in France and Germany is consistent with their identity shaped by World War II, the US preoccupation with free speech – at times at the expense of other widely recognised human rights – is embedded in the fact that 'the United States was a nation born of dissent and distrust of government institutions'.[157] In other words, these cases invariably concern issues which are not only reflective of national values but in fact go to the very heart of the State's identity and throw a shadow over competing concerns, such as overregulation of content providers and its implications for e-commerce or fairness to the individual and interstate relations.

5. The better path?

Online businesses are not allowed to hide wholesale behind contractually chosen legal regimes. Sometimes consumer protection provisions override these choices, and the criminal and other public laws of States are always lurking in the background. The critical question is the laws of which State will kick in. The above discussion shows that in both private and public law, the long arms of States have become longer with increasing globalisation. However, there are also important differences between the public and private approaches, both of which have pros and cons.[158]

See David Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd edn, Oxford: Oxford University Press, 2002), 764f.

[154] R 645–2 of the French Criminal Code and ss.130 and 131 of the German Criminal Code.

[155] Section 13(1) of the Canadian Human Rights Act and s.18C of the Racial Discrimination Act 1875 (Cth).

[156] For other examples, see Graham J. H. Smith, *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002), 525ff.

[157] For example, Laura R. Palmer, 'A Very Clear and Present Danger: Hate Speech, Media Reform, and Post-Conflict Democratization in Kosovo' (2001) 26 *Yale Journal of International Law* 179, 205, where the author provides a comparison between the German and US approaches to free speech and their backgrounds.

[158] Note the differences are one of degree. As considerations of enforcement jurisdiction have influenced the outcome in private matters (see e.g. the defamation case of *Macquarie Bank Ltd* v. *Berg* [1999] NSWSC 526) so the very existence of the effects doctrine in international law is evidence that jurisdiction may be asserted even in the absence of enforcement power and that fairness demands that States can regulate activity by which they are substantially affected.

The approach in private matters, as evidenced in both the EU and the US, seeks to provide fair and just results and thus requires a meticulous analysis, evaluation and balancing of facts and interests. The doctrinal adjustments in response to the Internet seek to accommodate the risks associated with too broad jurisdictional assertions (i.e. multiple concurrent claims and overregulation of online actors) by searching not simply for a link with the State *per se*, but a relatively strong link – relative in comparison to other possible links. In principle, this approach is correct and entirely consistent with the tradition of the allocation of regulatory competence. The pitfall though is that the decision-making process becomes more and more refined as jurisdiction is based on ever more subtler colour variations, which makes it harder to ensure consistency and formal justice. It illustrates that better rules are not necessarily to be found in the most refined and all-embracing, well-balanced rules and that at times legal principles which are not overtly sensitive to all the various interests at stake but clear-cut and thus capable of providing certainty and predictability, may in the final analysis be more just and desirable. It seems likely that, with the steady rise in transnational activity, highly refined jurisdictional rules will be sidelined in favour of, and become fall-back/niche options to, more easily administered mainstream solutions.

The second approach, as exemplified by recent transnational criminal cases, is less concerned with the overall fairness of the outcome as with protecting existing public interests, and thus involves a readiness to find a basis for asserting jurisdiction whenever its exercise is likely to be effective; in other words, holding on to the eggs in one's possession. In some ways, the lack of doctrinal developments in response to the Internet in respect of criminal jurisdiction is in terms of its propensity to provide certain, consistent and predictable outcomes and thus formal justice superior to those in private law. When in possession of enforcement power, States tend to exercise adjudicative jurisdiction (especially in respect of online activity which is contrary to their fundamental moral and cultural values) not only when the effects on the territory are intended and substantial, but upon the most tenuous basis. But the strict limits of enforcement jurisdiction to some extent temper the blanket application of the 'crude' effects doctrine.

Yet, the might-over-right approach is not without serious weaknesses. First of all, there is something decidedly regressive about 'a legal doctrine which sanctions the test of physical power ... [It is]

retrograde and parochial in character and should be firmly rejected.'[159] Furthermore, it fails on substantive justice grounds: it is just neither to States nor to individuals. When a State lacks enforcement jurisdiction, there is little it can do to protect its existing regulatory objectives, even in respect of online activity which has a significant effect on its territory. This probably affects most strongly States which have fewer local online providers and which are more reliant on foreign content. Also, the force of this approach will be felt by a few unlucky individuals or businesses, who happen to be within the enforcement reach of the State, while others get away with the same activities. In fact, the might-over-right approach encourages online content providers to minimise regulatory compliance cost by avoiding a presence, for example through a subsidiary, in targeted jurisdictions, opting instead for regulatory havens analogous to tax havens and flag-of-convenience States.

Ultimately, the discussion highlights that the allocation of regulatory competence on the basis of the location of persons, things or conduct is becoming increasingly difficult whatever approach one chooses. Just as colour ceased to be a useful concept in distinguishing between eggs, so location gradually passes its use-by date as a criterion for distinguishing between legally significant conduct. It cannot be too long before the allocation of regulatory competence based on location-centric concepts will tip. The traditional solutions to transnational events or a lack thereof were workable because these events were exceptional. When transnational events are commonplace, squeezing them into a system designed to handle the exceptional occurrence is highly inefficient. If non-primary coloured eggs had been as common as primary coloured eggs right from the outset, it seems inevitable that an industry dedicated to them would have developed alongside the other industries.

[159] F. A. Mann, 'Conflicts of Laws and Public Law' (1971) 132 *Recueil des Cours* 107, 121.

4

Many destinations but no map

1. Notice of foreign legal obligations

Online publications are often about people, and as it is perhaps human nature to find greater pleasure in writing and reading scandalous stories reflecting upon the wickedness of one's fellow men than about the Mother Teresas of this world, defamatory material abounds in cyberspace. Furthermore, given that the publishers of such stories, their victims and their readership are more often than not located in different States, a relatively substantial body of transnational defamation cases has built up. Perhaps by now not surprisingly, in these cases courts have struggled with the issue of how to accommodate transnational defamatory publications within the parameters of national defamation law – parallel to those discussions which have taken place in trademark law, consumer contract law and in the various areas of public or criminal law. Bar minor variations, the common themes running through these areas are undeniable. Again, in online defamation cases there is a strong judicial endorsement of the country-of-destination approach despite the protests of the online publishing community and many persuasive arguments to the contrary. Again, there is a tension between the moderate country-of-destination approach (concerned with the protection of online publishers from overregulation) and the outright country-of-destination approach (concerned with the protection of online 'consumers' from injurious foreign content). In this chapter, the country-of-destination approach moves centre-stage. The chapter discusses what is identified as the main challenge to the country-of-destination approach, namely, notice: the ability of online publishers to foresee and know their foreign legal obligations. The question addressed is: to what extent is the imperative of notice reconcilable with the country-of-destination approach? Again, the discussion is still primarily concerned with the regulatory claims States make in principle (adjudicative and legislative jurisdiction) and not with the question of whether those claims can in fact be enforced (enforcement jurisdiction), which is explored in Chapter 6.

Defamation provides an ideal illustration of the pitfalls of the country-of-destination approach in the online context and of possible solutions – partly simply by virtue of the fact that judges have had to confront it head on[1] (and for once not mainly from the US[2]). This is based on the fact that, in transnational defamation cases, adjudicative and legislative jurisdiction (or, in the language of private international lawyers, jurisdiction and choice of law) are often tightly intertwined. Under English and Australian common law, for example, whether a transnational defamation dispute should be heard in the forum is decided mainly by reference to the location of the defamation,[3] which also provides the test

[1] There is a substantial body of secondary literature on the topic. A few select examples: Matthew Collins, *The Law of Defamation and the Internet* (2nd edn, Oxford: Oxford University Press, 2006); UK Law Commission, *Defamation and the Internet – A Preliminary Investigation*, Scoping Study No. 2 (December 2002), esp. Part IV, www.lawcom.gov.uk/docs/defamation2.pdf; Oren Bigos, 'Jurisdiction over Cross-Border Wrongs on the Internet' (2005) 54 *International and Comparative Law Quarterly* 585; Richard Garnett, 'Dow Jones & Company Inc. v. Gutnick – An Adequate Response to Transnational Internet Defamation?' (2003) 4 *Melbourne Journal of International Law* 197; David Rolph, 'The Message, Not the Medium: Defamation, Publication and the Internet in Dow Jones & Co. v. Gutnick' (2002) 24 *Sydney Law Review* 263; Damjan Mozina, 'Persönlichkeitsverletzungen im Internet – Die Internationale Zuständigkeit' (2004) 1 *Slovenian Law Review* 77; Holger P. Hestermeyer, 'Personal Jurisdiction for Internet Torts: Towards an International Solution' (2006) 26 *Northwestern Journal of International Law and Business* 267. My own papers on various aspects of online defamation: 'Ignorance Is No Defence But Is Inaccessibility? On the Accessibility of Law in the Transnational Online Context' (2005) 14 *Information and Communications Technology Law* 27; 'Who Has the Right to Govern Online Activity? A Criminal and Civil Point of View' (2004) 18 *International Review of Law, Computers and Technology* 387; 'Defamation on the Internet – Nice Decision, Shame about the Reasoning: Dow Jones & Co. v. Gutnick' (2003) 52 *International and Comparative Law Quarterly* 1049; 'Defamation on the Internet – A Duty Free Zone After All? Macquarie Bank Ltd & Anor v. Berg' (2000) 22 *Sydney Law Review* 119.

[2] The First Amendment to the US Constitution makes it difficult to succeed with defamation actions in the US, and thus quite a few Internet cases which might otherwise have arisen in the US shifted elsewhere: *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56; *Harrods Ltd* v. *Dow Jones & Co. Inc.* [2003] EWHC 1162 (QB); *Lewis* v. *King* [2004] EWCA Civ 1329 (CA).

[3] Note that the location of the tort in the forum tends to be only one of a number of heads upon which a court can rely to found personal jurisdiction over the foreign defendant. But, at the next *forum non conveniens* inquiry, there is a general presumption that the natural forum in which to try the dispute is where the tort was committed: *Berezovsky* v. *Michaels* [2000] 1 WLR 1004, 1013f; following *The Albaforth (Cordoba Shipping Co. Ltd* v. *National State Bank, Elizabeth, New Jersey)* [1984] 2 Lloyds's Reports 91, 96; see also *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 47f. In the US, the inquiry on personal jurisdiction is not as obviously linked to the choice of law inquiry. But as personal jurisdiction over the foreign defendants is generally established on the basis of

for the substantive law governing the tort.[4] This close interrelationship has had a significant impact on the type and tenor of arguments advanced by the parties and courts in online defamation cases. The reason is that, if the issue is 'only' one of adjudicative jurisdiction and clearly separate from the applicable law, the main concerns underlying the arguments are those of procedural fairness to both parties, relative practicalities, cost and convenience.[5] Adjudicative jurisdiction has, at least in principle, no bearing on which substantive law governs the case and thus its outcome and substantive justice; whether the dispute is heard here or there, in theory the choice-of-law rules should yield the same substantive law and thus the final result should be the same.[6] This general theoretical assumption has meant that adjudicative jurisdiction has always tended to be more expansive than legislative jurisdiction, justifiable by weaker links with the State.[7] Most private international law regimes operate on the assumption that in respect of most civil disputes a number of courts could conceivably be appropriate fora to hear the matter. In contrast, only one set of substantive laws can govern each

special jurisdiction, it is necessary to show that the 'minimum' contacts with the forum are those which gave rise to the particular cause of action. This invariably means that the cause of action arose in the forum, which in turn means that the substantive law applied to the case is also forum law.

[4] In Australia, only recently adopted: *Regie National des Usines Renault SA* v. *Zhang* (2002) 76 ALJR 551. See also Bigos, above n. 2, 604, where the author argues that the *lex loci delicti* should be interpreted differently for the jurisdiction and for the choice-of-law inquiry. This seems to complicate unnecessarily an already highly technical area of law, and judicial practice does not support that differentiation.

[5] Nevertheless in reality 'jurisdiction' is often decisive and, once decided, cases are often settled out of court. Bigos, above n. 2, 587. 'No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet' (2003) 116 *Harvard Law Review* 1821, 1824f (note).

[6] The reality is very different: Andrew Beech, 'Discretion in the Exercise of Jurisdiction: Recent Developments' (1989) 19 *Western Australian Law Review* 8, 21, where the author notes that beyond the practical burden on one of the parties of having to litigate abroad, the place of litigation often significantly affects the substantive outcome given (1) the application of forum law to procedural matters e.g. quantification of damages, (2) the application of forum choice-of-law rules, (3) the potential exposure to forum mandatory laws irrespective of the applicable law according to ordinary choice-of-law principles. Michael C. Pryles, 'Internationalism in Australian Private International Law (1989) 12 *Sydney Law Review* 96, 106, where the author refers to the homeward trend of judges, i.e. 'a natural tendency on the part of judges and lawyers to prefer their own laws and legal institutions to those of foreign countries'.

[7] For example, in many Commonwealth countries adjudicative jurisdiction may be based on the damage suffered in the forum, even if the wrong was committed elsewhere.

dispute.[8] So, in the online context, in legal areas where adjudicative and legislative jurisdiction are more clearly separate inquiries, even a weak nexus adopted for adjudicative jurisdiction can be, and has been, defended on the basis that it does not necessarily expose online publishers to innumerable substantive laws; that is a different issue. Typically, the consumer provisions in the EC Jurisdiction Regulation[9] (which in the opinion of the author provide a strong connection) have been defended along those lines:

> [T]he Jurisdiction Regulation only regulates international *jurisdiction* in civil and commercial matters involving cross-border activities and elements, not issues of choice of law. The choice of law in consumer contracts is regulated by the Rome Convention, so it is incorrect to maintain that the consumer provisions in the Jurisdiction Regulation will make e-commerce retailers subject to fifteen different consumer *laws*.[10]

While this argument is not entirely persuasive,[11] it certainly carries no weight in those transnational defamation cases where adjudicative and legislative jurisdiction go hand in hand.[12] In these cases, courts could not avoid facing squarely the issue as to what can reasonably be expected of online providers in terms of compliance with foreign law. Can they be expected to know and comply with the laws of all the States where their sites are accessible, or only of those States which were specifically targeted by them or, perhaps going even further – as online publishers have argued – only with the laws of the one State from which their site originates? Online defamation brings into sharp focus one of the most central issues in the Internet governance debate which ultimately underlies most, if not all, legal areas affected by the transnationality of the Internet: the laws of which States should online actors comply with? What can reasonably be expected of them?[13]

[8] There are exceptions, as, for example, when a contractual choice of the applicable law is partly upheld and partly supplementary by mandatory rules of the forum.

[9] Art. 15(1)(c) of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001.

[10] Joakim S. T. Oren, 'International Jurisdiction over Consumer Contract in e-Europe' (2003) 52 *International and Comparative Law Quarterly* 665, 667 (internal footnotes omitted, emphasis in the original).

[11] See above n. 6; and also *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations*, COM(2005) 650 final, which in respect of consumer contracts follows the approach taken in the EC Jurisdiction Regulation.

[12] See above n. 3.

[13] Defamation cases have arguably raised this question with even more urgency than the transnational online criminal cases where the discussion remains more theoretical

This question exposes the main substantive competing interests operating in this field: on the one hand, States have an interest in protecting their residents (through the provision of private actions and criminal prosecutions) from 'harmful' foreign Internet activity (as defined differently in different States). On the other hand, online publishers have an interest in being able to order their affairs in accordance with the law[14] – a matter in which States themselves should have a significant interest as it is vital for both the legitimacy and the effectiveness of their laws. But online publishers can order their affairs in accordance with the law if, and only if, first, the law's application is foreseeable, and, secondly, they actually foresee and know it. In the Internet context, either may be difficult – depending on the type of country-of-destination approach adopted by States. If an outright country-of-destination approach is adopted, a law's application is easily foreseeable:[15] the laws of every State where the site can be accessed, which is often every State. But actually foreseeing, knowing and ultimately complying with those laws is practically impossible.[16] That problem is avoided, or ameliorated, if a more moderate country-of-destination approach is adopted. Then fewer legal regimes apply, but can they be foreseen? Also, are States happy to forego competence when a site has an effect, albeit minor, within their territory? But let us start at the beginning.

2. Foreseeability of foreign defamation law

A. Foreseeability and the rule of law

In most legal systems, there pertains the maxim that ignorance of the law is no defence. Regardless of whether or not you actually knew the legal

than real, given that there is no prospect at all of enforcing State assertions of adjudicative/legislative jurisdiction over foreign actors. But, even in defamation cases, there is often no willingness to enforce foreign judgments, especially in the US: see Jeremy Maltby, 'Juggling Comity and Self-Government: The Enforcement of Foreign Libel Judgments in US Courts' (1994) 94 *Columbia Law Review* 1978; Jeff Sanders, 'Extraterritorial Application of the First Amendment to Defamation Claims against American Media' (1994) 19 *North Carolina Journal of International Law and Commercial Regulation* 515.

[14] The general assumption made in this chapter is that online actors on the whole would prefer to act legally irrespective of whether they could be forced to do so.

[15] On the difficulty of actually foreseeing foreign legal rules, see section 4 below.

[16] Such compliance would only in rare instances be logically impossible: when the law of one State requires what the law of another State forbids. Generally, the most common 'conflicts' are where one State imposes a more stringent duty than another State, which means that the publisher can comply with both laws by complying with the more stringent one.

consequences of your actions you may be held legally accountable for them. It is a fair maxim. It prevents individuals from relying on their ignorance to avoid responsibility, which would reward the ignorant while punishing the knowledgeable. It also creates an incentive for individuals to familiarise themselves with their legal obligations.

While this is fairly uncontroversial, the maxim cannot be seen in isolation from another feature of any legal system which seeks to uphold the rule of law. There must not be secret laws: legal consequences must be foreseeable – not necessarily foreseen in the particular case but foreseeable in principle. Individuals should only be accountable for their actions if they could know – if they wished to – the legal consequences attaching to alternative courses of conduct. They must have had the opportunity to choose whether to comply or take the risk of sanctions for non-compliance. Or, more formally, the rule of law entails that 'people should obey the law and be ruled by it'.[17] For people to obey the law,

> the law must be capable of being obeyed. A person conforms with the law to the extent that he does not break the law. But he obeys the law only if part of his reason for conforming is his knowledge of the law. Therefore, if the law is to be obeyed *it must be capable of guiding the behaviour of its subjects*. It must be such that they can find out what it is and act on it.[18]

What does this entail for legal rules and a legal system? It broadly entails three matters. First, there must be signposts, i.e. warning mechanisms, which put people on notice about the legally significant nature of their activities and alert them to the possible legal consequences of their actions. Secondly, individuals must be able to actually access the relevant legal resources: 'Elementary justice ... demands that the rules by which the citizen is to be bound should be ascertainable by him (or more realistically, by a competent lawyer advising him) by reference to identifiable sources that are publicly accessible.'[19] As will be seen below, all legal systems rely on much more informal methods to both warn and inform legal subjects of their rights and obligations. Thirdly, the rules themselves must be such that they are capable of guiding behaviour. Raz argues that this requires that all laws must be prospective, unambiguous, clear and relatively stable, both for

[17] Joseph Raz, 'The Rule of Law and its Virtue' (1977) 93 *Law Quarterly Review* 195, 196.
[18] *Ibid*., 198.
[19] *Fothergill* v. *Monarch Airlines* [1981] AC 251, 279 (HL). See also McMahon, 'Improving Access to the Law in Canada' [1999] *Computerisation of Law Resources* 3.

short- and long-term decision-making.[20] These are basic requirements designed to protect human dignity and autonomy which 'entails treating humans as persons capable of planning and plotting their future'.[21] They are not mere niceties or pretty decorative touches attaching to legal systems, but reflect fundamental values which most States, and in particular Western democratic societies, claim to treasure. The critical question is to what extent individuals acting on the global Internet can order their affairs with relative legal certainty, given their exposure to numerous foreign laws.[22]

B. Absence of noticeable borders in cyberspace

If online publishers do not know who actually accesses their site or who might access their site, but nevertheless that access or accessibility is in law treated as the critical nexus or link which exposes the publisher to the law of the surfer's State, then that foreign law is unforeseeable. The issue of foreseeability was foreshadowed by Johnson and Post, who argued that cyberspace removes the signpost function of physical borders,[23] which traditionally alerted individuals to the new legal space they had just entered. They argued that such borders simply do not exist on the Internet. Thus, '[i]f someone acting in any given space has no warning that the rules have changed, the legitimacy of any attempt to

[20] Raz, above n. 17, 198f. Where law is applied retrospectively, this is often justified by recourse to arguments based on natural law. H. L. A. Hart, *The Concept of Law* (2nd edn, Oxford: Clarendon Press, 1994), 208: 'It is in this form that Natural Law arguments were revived in Germany after the last war in response to the acute social problems left by the iniquities of Nazi rule and its defeat'; Deryck Beyleveld, Richard Kirkham and David Townend, 'Which Presumption? A Critique of the House of Lords' Reasoning on Retrospectivity and the Human Rights Act' (2002) 22 *Legal Studies* 185, 190f.

[21] Raz, above n. 17, 204.

[22] For a discussion of the rule of law in the context of competence, see Brian R. Opeskin, 'The Price of Forum Shopping: A Reply to Professor Juenger' (1994) 16 *Sydney Law Review* 14.

[23] David R. Johnson and David Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1357, 1375. See also *ACLU* v. *Reno*, 929 F Supp 824, 859ff (ED Pa 1996); Hague Conference on Private International Law (Avril D. Haines), *The Impact of the Internet on the Judgments Projects: Thoughts for the Future*, Prel. Doc. No. 17 (2002), 18: 'In addition to the problems faced with regard to identifying where the "act or omission" causing the injury occurred and where the injury "arose", a defendant would have difficulty, given the nature of the Internet, in proving that it was not "foreseeable" . . . that someone would be able to pull up the content of his or her web page in any country. Either every jurisdiction is foreseeable or no jurisdiction is foreseeable.'

enforce a distinctive system of law is fatally weakened. No geographically based sovereign could plausibly claim to have jurisdiction over a territory with secret boundaries.'[24] But is this really the case? It is argued below that the judiciary is not insensitive to the need for foreseeability which is often incorporated into legal doctrines through the requirement of a mental element.

However, those mental elements which indirectly import the requirement of foreseeability of legal exposure can be, and have been, interpreted in two different ways. On the one hand, the critical intentional act is taken to be entering cyberspace and that entry ought to alert online publishers to the applicability of the laws of all the States where the site can be accessed. Therefore, there is no further need for signposts within cyberspace itself, which would alert publishers of their entry into particular States. The laws of all States ought to be foreseen. On the other hand, the mere entry into cyberspace is not taken to be sufficient to expose online publishers to any or all laws. Publishers ought to foresee only the laws of the States which they target. Their own online activities directed at one State rather than another provide the necessary 'signposts' which ought to alert them to the particular law-space they enter.

The problem of notice is particularly acute in the online defamation context. First of all, defamatory sites are often not interactive, or only marginally so. Most major newspapers have an online version which caters for a passive readership; they are not primarily designed as platforms for online transactions, but simply to be read. Actual transactions are useful for notice purposes, because they often alert publishers to the whereabouts of their customers and also give them a chance to avoid contact with certain States. For this reason, these *knowing* online transactions figure highly in the *Zippo* test (personal jurisdiction in the US[25]) and the 'directing' test (personal jurisdiction in EU consumer contracts[26]). But what is to be done in respect of transnational online defamation when there are no knowing contacts with forum residents? Does the absence of indicia alerting website operators as to the whereabouts of their clientele undermine the legitimacy of any country-of-destination approach in the defamation context? Also, as a

[24] Johnson and Post, above n. 23, 1379 (n. 33).

[25] *Zippo Manufacturing Co.* v. *Zippo Dot Com Inc.*, 952 F Supp 1119 (WD Pa 1997).

[26] Art. 15(1)(c) of the EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001; see Chapter 3, section 2.A, above.

side note, transnational defamation may also arise out of online publications which are not commercial such as, for example, blogs, personal homepages or chat-rooms,[27] which makes the no-pain-no-gain maxim – also underlying the US *Zippo* test and the EU 'directing' test – not as obviously helpful in understanding how the law should develop to accommodate online transnational defamation. Neither can defamation law benefit from contractual choice; in contract law, foreign law or courts can be easily foreseen when the contractual parties choose it and that choice is upheld. So defamation law provides an ideal testing ground for exploring the issue of notice.

At the most basic level, the cases below highlight that the lack of harmonisation in private international law exacerbates the problem of the foreseeability of legal exposure.[28] Online content providers have to not only absorb the differences in the substantive laws on defamation, but also cope with different rules as to when these substantive laws apply. However, despite differences in the specific rules, there are certainly common themes in the approach. The following examines how States, particularly common law jurisdictions, have dealt with transnational online defamation.

C. Actual access, even if minuscule

For a civil defamation claim to succeed, English and Australian common law requires, first, that there was a 'publication' of the defamatory statement to a third party which takes place where the statement is heard or comprehended.[29] Secondly, that 'publication' need not be

[27] Adam Sherwin, 'Chat Room Insults Lead to Internet Libel Victory' (22 March 1996), *The Times* (UK), 17.

[28] For harmonisation efforts in the EU, see *Amended Proposal for a European Parliament and Council Regulation on the Law Applicable to Non-Contractual Obligations (Rome II)*, COM(2006) 83 final. Differences of the rules are described in the initial *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations (Rome II)*, COM(2003) 427 final, 5f, 17f.

[29] In common law countries, see *Bata* v. *Bata* (1948) WN 366; *Lee* v. *Wilson and Mackinnon* (1934) 51 CLR 276. Note that, despite some minor variations, all EU States apply the law of the State where the defamatory statement has been distributed and where the victim enjoys a reputation. In some States this rule provides an alternative to the law of the State where the publisher is established; in the UK, the law of the location of the defamatory publication only applies if the publication occurred in the UK, otherwise the 'double actionability rule' applies. See *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations (Rome II)*, COM(2003) 427 final, 17f.

substantial; it is sufficient if it is made to a single third party. In the case of mass media, each separate publication of the same statement founds a separate cause of action.[30] These two rather simple propositions have translated in the transnational online context into another simple proposition: a website must have been actually accessed in the forum to found a local defamation claim, but a single hit on a foreign website satisfies the 'publication' requirement. The cases below illustrate this proposition as well as its rather drastic consequences for competence.

In *Dow Jones & Co. Inc.* v. *Gutnick*,[31] decided by the High Court of Australia, an Australian businessman alleged that Dow Jones, a US publisher, had defamed him in Australia in its magazine and its fee-paying subscription website. Both publications were largely aimed at the US market, but a few of the relevant magazines had been sold in Victoria and similarly the relevant website of *Barrons Online* had hits 'probably in excess of 300'[32] from Victoria. Despite the fact that this represented only a minuscule percentage of the overall number of readers, the High Court refused a stay of proceedings, holding in favour of the local court and local defamation law.[33] Both issues hinged on the location of the defamatory publication. The point of contention was whether a website is 'published' for defamation purposes in the place where it was uploaded onto the web (here, New Jersey (US)) or in the place where the subscribers accessed it (here, Victoria (Australia)). In practical terms, the issue was whether online publishers have to comply with the laws of the

[30] *Duke of Brunswick and Luneberg* v. *Harmer* (1849) 14 QB 184. In as much as holding on to the traditional concept of publication in the online environment entails the legal exposure of content providers across States, it also entails their repeat liability over time: *Loutchansky* v. *The Times Newspapers Ltd* [2001] EWCA Civ 1805. Contrast the US position under the 'single publication rule': *Firth* v. *The State of New York*, 775 NE 463 (Ct App 2002).

[31] [2002] HCA 56, affirming *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305 (Hedigan J). For the transcript of the arguments brought before the court, see *Dow Jones & Co. Inc.* v. *Gutnick* M3/2002 (28 May 2002), www.austlii.edu.au. Australian Standing Committee of Attorney-Generals (SCAG) Working Group of State and Territory (NSW) Officers, *Proposal for Uniform Defamation Laws* (July 2004), 34f, noting that no legislative change is required following *Gutnick*. The earlier English case of *Berezovsky* v. *Michaels* [2000] 1 WLR 100 also involved an Internet publication in addition to a magazine, but the House of Lords reached its decision without considering the online publication.

[32] *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305, para. 32.

[33] The three interrelated inquiries were set out most clearly by Kirby J in *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 93–110: (1) did the Victorian court have jurisdiction to hear the dispute (2) was it a *forum non conveniens* and (3) was Victorian defamation law the applicable law?

single place from where the activity originates (i.e. the country of origin) or with the laws of *all* the places of their customers (i.e. the countries of destination).[34] The High Court unanimously rejected the country-of-origin approach to online defamation and upheld the traditional position that a defamatory publication occurs where the publication is comprehended and not where it is composed.[35] The link which creates competence is actual access, even if minimal, as in this case.[36]

Similarly, in *Harrods Ltd* v. *Dow Jones & Co. Inc.*,[37] again Dow Jones was sued by Harrods Ltd in respect of an article (following a Harrods' April Fools joke) which appeared in the US, but not the European, edition of its *Wall Street Journal* and its website, for defaming the company in the UK.[38] The evidence showed that its US edition had been sent to ten subscribers in the UK (compared to the 1.8 million copies sold in the US) and similarly the website had a few hits from the UK. Despite the minuscule distribution on English soil, the court still found in favour of the English court and law, as the victim was an English company with a well-established reputation in England.[39] The defendant did argue that the distribution was simply too minuscule and too technical to count, but this argument was unsuccessful.[40] One may very well wonder when, if ever, the second proposition noted in *Lewis* v. *King*[41] kicks into play:

> the starting-point for the ascertainment of what is clearly the most appropriate *forum* is to identify the place where the tort has been committed . . .

[34] On appeal to the High Court, several high-profile publishers, including Amazon.com, Yahoo! Inc., the New York Times Company and Guardian Newspapers Ltd, were granted leave to intervene. Many of them were from the US, whose relatively publisher-friendly laws mean that they have most to gain from a country-of-origin approach. See *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 188–90 (Callinan J) on the fundamental differences of US and Australian/English defamation law.

[35] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 44, 151, 197ff.

[36] And Kirby J specifically rejected any middle-ground whereby only target destinations should count: *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 131.

[37] [2003] EWHC 1162 (QB). For Dow Jones' unsuccessful attempt in the US to stall the UK proceedings, see *Dow Jones & Co. Inc.* v. *Harrods Ltd and Mohamed Al Fayed*, 237 F Supp 2d 394 (2002).

[38] Although it seems that the action in England was in reality designed to vindicate Harrods' reputation worldwide: *Harrods Ltd* v. *Dow Jones & Co. Inc.* [2003] EWHC 1162 (QB), paras. 5, 9.

[39] *Harrods Ltd* v. *Dow Jones & Co. Inc.* [2003] EWHC 1162 (QB), para. 44.

[40] Relying on *Kroch* v. *Rossell* [1937] 1 All ER 725, requiring a real and substantial connection to found jurisdiction.

[41] [2004] EWCA Civ 1329 (CA).

> But – and here is our second proposition from the cases – the more tenuous the claimant's connection with the jurisdiction (and the more substantial any publication abroad), the weaker this consideration becomes.[42]

Clearly, even a minuscule distribution out of the overall distribution may not preclude the forum court from asserting adjudicative competence.

In Canada, a minuscule publication (two hits from Canadian surfers) did not deter the court in *Kitkufe* v. *Olaya Ltd*[43] from refusing to grant a stay of proceedings[44] concerning an alleged defamatory article in a newspaper published in Uganda but re-published online, and alleged to have injured the plaintiff's reputation in Canada. Although there was a number of factors which connected the dispute to Canada,[45] the fundamental basis upon which *forum non conveniens* even became an issue was the two hits from Canadian territory. The same approach of focusing on actual access has also been adopted in Malaysia[46] and in a criminal defamation case in Italy.[47]

Of course, the problem of multiple simultaneous publications is not peculiar to the Internet and has caused problems for all mass media, whether books, magazines, television or radio.[48] The traditional stance is that it does not matter that the bulk of the distribution occurred

[42] *Lewis* v. *King* [2004] EWCA Civ 1329 (CA), para. 27.

[43] ACWSJ LEXIS 84447 (Ontario Court of Justice, 1998), 11f: 'I am mindful of the defendant's position that the alleged defamatory article was only published in Uganda and that access on the Internet was limited to two people in Ontario and only to parts of the newspaper other than the page where the article occurred.' So, strictly speaking, there may not have been a 'publication'.

[44] The court applied the *forum non conveniens* test laid down by the House of Lords in *MacShannon* v. *Rockware Glass Ltd* [1978] 1 All ER 625, according to which the defendant must show that there is not a substantially more convenient court where the claim can be adjudicated.

[45] *Kitkufe* v. *Olaya Ltd*, ACWSJ LEXIS 84447 (Ontario Court of Justice, 1998), 10; for example, the defendant and many witnesses were not resident in Canada.

[46] *Lee Teck Chee* v. *Merrill Lynch International Bank Ltd* [1998] Current Law Journal 188, 194f, although in this case the issue is somewhat complicated by the fact that the High Court of Malaysia decided that there was no evidence of publication because they did not have the requisite permission to be imported, sold, distributed or circulated in Malaysia. This of course does not necessarily mean that they were not in fact published in Malaysia.

[47] *Re Moshe D* (Italian Court of Cassation, 17 December 2000), www.cdt.org/speech/international/20001227italiandecision.pdf.

[48] *Jenner* v. *Sun Oil Co*. [1952] 2 DLR 526 (radio); *Pinding* v. *National Broadcasting Corp*. (1985) 14 DLR (4th) 391 (television).

elsewhere. In the English case of *Berezovsky* v. *Michaels*,[49] a Russian businessman sued a US magazine in England on the basis of a few copies (0.2 per cent of the total circulation) which had been distributed in England. The House of Lords decided that England was the appropriate forum, principally because the tort had been committed in England through the distribution of the magazine where the plaintiff had a reputation to protect.[50] It did not matter that the UK was not targeted. Lord Steyn rejected the targeting approach (focusing on the location of the bulk of the publication) as inconsistent with established principles of libel law.[51] All that mattered was that some magazines had been distributed in the UK.

The parallels between this scenario and the online scenario are unmistakable. And yet, one may question whether the online scenario is not after all distinguishable from the offline scenario. Is the circulation of newspapers in certain States not *quantitatively* different from allowing hits on one's website? Online it is much easier to 'circulate' *fewer* copies to *many more* States.[52] *Prima facie* this does not affect matters of principle, but it does make it questionable whether a position that entitles any country of destination to assume competence, no matter how few hits, is still fair and strikes the correct balance between publishers and defamed plaintiffs.

Even in the US, courts have consistently focused on the destination of publications and equally have *prima facie* treated even small publications as giving rise to a defamation – despite the US 'single publication rule'.[53] The 'single publication rule' is at best marginally relevant to competence questions.[54] It was[55] designed to be no more than a procedural device, applicable where the plaintiff has suffered damage in a

[49] [2000] 1 WLR 1004. [50] *Berezovsky* v. *Michaels* [2000] 1 WLR 1004, 1013.
[51] *Ibid.*, 1012f. [52] See Chapter 2.
[53] §577A of the US Restatement (Second) of Torts (1977).
[54] Rejected as irrelevant in *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 35, 65; also rejected in *Berezovsky* v. *Michaels* [2000] 1 WLR 1004, 1011: 'The Uniform Single Publication Act does not assist in selecting the most suitable court for the trial: it merely prevents a multiplicity of suits.' See also *Loutchansky* v. *The Times* [2001] EWCA Civ 1805. Note also that the US 'single publication rule' is an exception to the main rule, according to which each communication by the same defamer, whether to a new person or to the same person, is generally a separate publication giving rise to separate causes of actions: see §577A of the US Restatement (Second) of Torts (1977).
[55] For a brief description of the development of the rule and its frequent judicial convolution with choice of law and jurisdiction issues, see *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 29–35; or Law Commission, above n. 2, paras. 3.1ff.

number of States. The rule allowed a plaintiff to recover damages for all those injuries in one action, barring claims in other jurisdictions.[56] So it deals with a very specific scenario: not just with multiple publications of the same statement *per se*, but with multiple injuries arising out of these multiple publications. Its rationale is to prevent a multiplicity of suits in respect of the same defamatory statement. But it does not say where the single action should be brought and which law should be applied to it. In *Keeton* v. *Hustler Magazine Inc.*,[57] the Supreme Court held that the New Hampshire court had jurisdiction over a Californian defendant on the basis that the defendant had circulated some magazines in New Hampshire each month, although most of the damage had been suffered elsewhere. The court asserted that libel is generally held to occur wherever the offending material is circulated,[58] just as it was decided in England and Australia. For the single publication rule, *any* of the countries of destination where 'a substantial number of copies are regularly sold and distributed'[59] may be a suitable forum, not just the main target. By implication, if the damage is restricted only to one State, even a small circulation is sufficient to make the forum suitable, just like in Australia and England.[60]

Last but not least, Article 5(3) of the EC Jurisdiction Regulation[61] also accommodates this focus on actual hits on a foreign website from the forum. It provides that a defendant may be sued in the place where the 'harmful event occurred' which 'cover[s] both the place where the damage occurred and the place of the event giving rise to it'.[62] In the context of defamation, that first limb has been held to be the place where

[56] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 35. Other States use other mechanisms to stop multiple litigation in respect of the same publication. See e.g. s.9(3) of the Defamation Act 1974 (NSW) which prohibits more than one action in respect of multiple publications without leave of the court. Furthermore, plaintiffs may be prevented from bringing multiple actions in respect of the same publication on the basis of vexation. In the EU, multiplicity of suits was addressed in *Shevill* v. *Presse Alliance SA*, Case C-68/93 [1995] ECR I-415, para. 32: the victim must sue in the court of the State where the publisher is established if he wants to recover for the damage suffered in a number of States.

[57] 465 US 770 (1984).

[58] *Keeton* v. *Hustler Magazine Inc.*, 465 US 770, 777 (1984).

[59] *Ibid.*, 771.

[60] Which is precisely the reason why Gutnick restricted the damages through an undertaking to the court to sue in no place other than Victoria.

[61] EC Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 44/2001.

[62] *Shevill* v. *Presse Alliance SA*, Case C-68/93 [1995] ECR I-415, para. 20, following *Bier* v. *Mines de Potasse d'Alsace*, Case 21/76 [1976] ECR 1735, para. 11.

the plaintiff's reputation was harmed by virtue of third persons reading and comprehending the publication.[63] For online defamation, those are the places where the site has been actually accessed.[64]

So, although there is an insistence that the site in question has actually been accessed from the State, that access can be minimal. This means that competence is often asserted over foreign sites which have only a minimal effect on the State and that effect is very likely replicated in many States. The critical question in this context is: is there a legal requirement that the online publishers must have known or could have known the location of those who accessed his site? If the actual hits which trigger legal exposure are not known or preventable, then legal exposure itself cannot be known or prevented.

D. Foreseeability of foreign law in respect of freely accessible sites

Have courts been sensitive to the concern that an online publisher may not have known about the actual hits on his site? This matter was specifically raised in *Gutnick*: 'if the rule of law . . . is to have any social meaning, then . . . it will include the capacity to know it in advance so as to be able to shape your conduct in the light particularly of the deterrent example held out by people who have been ordered to pay damages . . . in the past.'[65]

As the site in question was a subscription website,[66] foreseeability should have been straightforward. The credit card details would generally and automatically have revealed the location of the subscribers. But the High Court of Australia did not attribute any legal significance to fee-paying subscription nature of the site. Kirby J suggested that in respect of both subscription and freely accessible sites it is impossible

[63] *Shevill and Others* v. *Presse Alliance SA* Case C-68/93 [1995] ECR I-415, para. 2.

[64] There are arguably some indications that the European Court of Justice may not take an expansive view on competence. In *Bodil Lindqvist*, Case C-101/01 [2004] 1 CMLR 20, the court held that the publication of personal data on a private website dedicated to the activities of a Swedish church did not amount to a 'transfer of data to a third country' pursuant to the EC Data Protection Directive, 1995/46/EC, even if such data are thereby made accessible to persons in third countries. Although the main reasons for this holding appears to have been that the Directive was drawn up when the Internet was in its infancy, it is significant that the court did not simply transplant traditional legal concepts to the online world in respect of its transnationality.

[65] *Dow Jones & Co. Inc.* v. *Gutnick*, M3/2002 (28 May 2002), 21, also 25f.

[66] The commercial nature of the site (relevant for the no-pain-no-gain maxim) was noted as significant by Callinan J in *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 182.

for the website operator to know with 100 per cent certainty the location of the readers[67] because of anonymising technologies or credit cards issued by a country not corresponding to the subscriber's country of residence. His implicit suggestions were, first, that there is no legally significant difference between the two different types of site, and, secondly, that 100 per cent accuracy is vital for legal purposes. Neither of these propositions is entirely persuasive.

In the context of a subscription website, generally the true location of the subscriber reveals itself through the credit card details, and applications from unwanted States can easily be excluded. Operators of freely accessible sites would have to take additional steps and adopt geo-location technology to know the location of surfers and exclude unwanted ones.[68] Of course, such sites would then by definition no longer be freely accessible sites. The difference between subscription and freely accessible sites is that with subscription sites selectivity is already part of the operation of the site and territorial selectivity falls neatly within it and does not substantially alter the structure of the site. Finally, because with subscription sites access is financially rewarded, there is less danger that legal exposure to foreign laws will discourage access and by implication valuable speech.

As to the matter of 100 per cent accuracy, should the online publisher accept a subscription in the reasonable, but mistaken, belief that the subscriber comes from a certain State, then the publisher should not be exposed to the laws of the subscriber's true location. This position is entirely consistent with traditional principles of defamation law according to which the publication (although not the defamation) must be intentional or negligent.[69] In the above scenario, there would be no intentional publication in the true location of the subscriber (and

[67] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 84.

[68] Dan Jerker B. Svantesson, 'Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet' (2004) 23 *John Marshall Journal of Computer and Informational Law* 101, 109ff: geo-location technology, based on matching IP addresses with location, is reasonably accurate and used for example by www.sho.com to exclude all but US users from accessing its site. In respect of subscription sites, see *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305, para. 73: 'Dow Jones controls access to its material by reason of the imposition of charges, passwords and the like, and the conditions of supply of material on the Internet. It can, if it chooses to do so, restrict the dissemination of its publication of Barrons on the Internet in a number of respects.' See also para. 115(11).

[69] John G Fleming, *The Law of Torts* (9th edn, Sydney: LBC Information Services, 1998), 599f.

therefore the tort would not have been committed there and therefore no legal exposure ensues). By the same token, in the standard case accepting online subscriptions, knowing the location of the subscribers entails that there is an intentional publication in those locations. Hedigan J at first instance[70] was sensitive to the requirement of intention. He addressed foreseeability as follows: '[i]t is also absolutely clear that Dow Jones intended that only those subscribers in various States of Australia who met their requirements would be able to access them, and they intended that they should',[71] implicitly approving the plaintiff's argument that 'the publication of the article to persons in Victoria who read it was the intended natural and probable consequence of all the acts of the defendant'.[72] *Gutnick* could have been an easy case; instead it became an interesting one. As the High Court did not restrict its ruling to subscription websites, how did it accommodate foreseeability of legal exposure?

Foreseeability of all destinations[73]

The High Court went along a well-trodden path (although more well-trodden in public than private law); if you go online, worldwide legal exposure is foreseeable:

> no more or less ubiquitous than some television services. In the end, pointing to the breadth or depth of reach of particular forms of communication may tend to obscure one basic fact. However broad may be the reach of any particular means of communication, those who make information accessible by a particular method do so *knowing* of the reach that their information may have. In particular, those who post information on the World Wide Web *do so knowing* that the information they make available is available to all and sundry without any geographic restrictions.[74]

The High Court took a robust approach, according to which online publishers are *prima facie* taken to have targeted all States. It means that, once actual access to the site is established, no further evidence is needed as to the intention behind the publisher's conduct in the particular territory. The consequence is: the legal requirement of actual access does not *prima facie* limit the regulatory burden of online publishers at all. If a publisher does not, and perhaps cannot, know the location

[70] *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305, paras. 38f, 68, 73.
[71] *Ibid.*, para. 60. [72] *Ibid.*, para. 43.
[73] Same as the 'crude' effects test, discussed in Chapter 3, section 4.B, above.
[74] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 39 (emphasis added).

of the actual hits, it would have to – just in case – comply with all laws. Given the availability of location-sensitive site-meters,[75] even publishers of freely accessible sites could track the whereabouts of visitors, and thus know at least which foreign legal system might come into play. But, without implementing access restrictions, they could not prevent or reduce that legal exposure. The legal burden on these publishers would still be unlimited.

This 'robust' approach was recently endorsed by the English Court of Appeal in *Lewis* v. *King*,[76] where it held that any online 'global publisher should not be too fastidious as to the part of the globe where he is made a libel defendant'.[77] Addressing the defendant's argument that, 'for the purposes of *forum non conveniens* enquiries involving material published via the Internet, the intention of the defendant should be taken into account',[78] the court simply said:

> it makes little sense to distinguish between one jurisdiction and another in order to decide which the defendant has 'targeted', when in truth he has 'targeted' every jurisdiction where his text may be downloaded. Further, if the exercise required the ascertainment of what it was the defendant subjectively intended to 'target', it would in our judgment be liable to manipulation and uncertainty, and much more likely to diminish than enhance the interests of justice.[79]

The court did not reject as irrelevant the publisher's intention *per se*, just his 'subjective intention'. And in terms of an 'objective intention', the court argued that online publishers must be taken, in light of the nature of the Internet, to target all States. As will be argued below, this is not the only way to interpret the concept of 'objective intention' in the context of online activity; it can be, and has been, interpreted to require an overall assessment of the site in its surrounding circumstances to see which *particular* States the publisher objectively targeted.

The High Court of Australia sought to explain why its ruling was not quite as dramatic as it seemed; why the exposure to multiple sets of foreign laws was more theoretical than real. First, the court pointed to the unlikelihood of having to defend defamation actions if the enforceability of any judgment was questionable.[80] Of course, this argument did

[75] For example, http://sitemeter.com.

[76] *Lewis* v. *King* [2004] EWCA Civ 1329 (CA), para. 31.

[77] *Ibid*., para. 31. [78] *Ibid*., para. 33. [79] *Ibid*., para. 34.

[80] *Dow Jones & Co. Inc*. v. *Gutnick* [2002] HCA 56, para. 53. The US has been very reluctant to enforce foreign defamation judgments against local publishers, applying the First Amendment to the US Constitution to those foreign publications; see above n. 13.

not deter Berezovsky, Gutnick, Harrods Ltd or King. Especially in defamation, the verdict itself may often be more important than any monetary compensation to vindicate the plaintiff's reputation. In any event, it seems unfortunate to justify the breadth of liability by reference to its frequent ineffectiveness. Should online publishers really be encouraged to flout the laws of States that cannot catch them? Again, Hedigan J adopted a more desirable stance when noting (albeit in relation to the risk of unenforceability of the judgment in the particular case) that the law should *prima facie* assume that the defendant will honour its legal obligations. The issue of enforceability becomes 'relevant [only] if the defendant declines to honour any judgment obtained which would be an improper course and damaging to the defendant's reputation worldwide'.[81] Secondly, the High Court suggested that online publishers can foresee the particular foreign laws by foreseeing the likely harm in the particular situation. To this argument we turn now.

Foreseeability of foreign harm

The High Court argued that in defamation cases it is easy to identify the particular laws which may come into play. All online publishers have to do is to look at the person who is the subject of the article and his residence, and this will determine which laws apply:

> the spectre which Dow Jones sought to conjure up in the present appeal, of a publisher forced to consider every article it publishes on the World Wide Web against the defamation laws of every country from Afghanistan to Zimbabwe is seen to be unreal when it is recalled that in all except the most unusual of cases, identifying the person about whom material is to be published will readily identify the defamation law to which that person may resort.[82]

Even more explicitly, Kirby J stressed that '[u]nlike product liability or some other negligence claims, damage to reputation cannot occur "fortuitously" in a place outside of the defendant's contemplation'.[83] In short, they held that defamation is different from other causes of action: in defamation, the location of the potential harm is foreseeable and thus the corresponding foreign law is also foreseeable.[84]

[81] *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305, para. 115(7).
[82] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 54, 134.
[83] *Ibid.*, para. 151.
[84] 'Damage in the forum' is a head of jurisdiction, rather expansive, in many Commonwealth countries, which has been criticised for being too insubstantial a link

In *Harrods Ltd* v. *Dow Jones & Co. Inc.*,[85] foreseeability was not specifically addressed, presumably because the printed journal had also been distributed in the UK; thus Dow Jones could hardly argue that it did not know about its destination. However, given how minuscule the distribution was, Dow Jones had not foreseen English legal exposure.[86] Yet, despite that, competence was asserted, first and foremost because the victim was an English company with a well-established reputation in England.[87] So, just like in *Gutnick*, the nationality or residence of the person defamed, in addition to the publication however minuscule, ought to have put Dow Jones on notice of English defamation law. In terms of foreseeability, this is noteworthy because it shows that foreseeability does not reflect what the particular defendant actually foresaw or even what an ordinarily diligent defendant in the circumstances might have foreseen; it is a legal decision as to what the defendant ought to have foreseen or is expected to foresee.

The location of the harm (i.e. of the plaintiff and his reputation) is a relatively stable factor where the plaintiff is an ordinary person, who lives in one State and enjoys a reputation only there. But what about internationally known figures? In *Lewis* v. *King*,[88] King, a US national with a worldwide reputation, sued Lennox Lewis (a British national, but resident mainly in the US) and two others alleging that two online publications had damaged his reputation in the UK. The sites had been very popular in the UK,[89] but the main injury had no doubt occurred in the US. He chose England, and not New York, to bring the action, because the 'public figure' doctrine would have doomed any US action.[90] So King's worldwide reputation, coupled with the worldwide availability of the site, allowed him to choose the most favourable forum. Where does that leave the online publisher? It certainly weakens the *Gutnick* argument that the location of potential litigation can easily be anticipated by reference to the subject of the article. In King's case, that was anywhere.

(e.g. *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, paras. 100f). If the *forum non conveniens* test is meant to act as a limiting device on expansive heads of jurisdiction, reference to the damage makes little sense in this inquiry. See also the discussion in Garnett, above n. 2, 202ff.

[85] [2003] EWHC 1162 (QB).

[86] Relying on the case of *Kroch* v. *Rossell* [1937] 1 All ER 725.

[87] *Harrods Ltd* v. *Dow Jones & Co. Inc.* [2003] EWHC 1162 (QB), para. 44.

[88] [2004] EWCA Civ 1329 (CA), affirming *King* v. *Lewis* [2004] EWHC 168 (QB).

[89] *King* v. *Lewis* [2004] EWHC 168 (QB), para. 26.

[90] *King* v. *Lewis* [2004] EWHC 168 (QB), para. 37; *Lewis* v. *King* [2004] EWCA Civ 1329 (CA), paras. 40f.

Last but not least, the EU also seems to be moving towards a damage-focused approach in its proposal to harmonise the law applicable to non-contractual obligations (commonly known as Rome II). There the general default rule provides that 'the law of the country in which the damage arises' furnishes the applicable law in tort disputes.[91] Yet, it is reasonably clear that this wording was chosen as a means of avoiding the interpretation of 'harmful event' in Article 5(3) of the EC Jurisdiction Regulation.[92] As noted above, 'harmful event' is there taken to refer both to the place of the initial act and to the place where that act took effect. Rome II is opting for the second limb only (stating expressly that the location of the initial act is irrelevant) and thus uses the perhaps slightly misleading reference to the location of the 'damage'. In fact, 'damage' does not refer exclusively to the harm suffered but also to the effect of the defendant's action. As stated in *Shevill* v. *Presse Alliance SA*, it is the law of the 'State in which the publication was distributed and where the victim claims to have suffered injury to his reputation'.[93] So the focus is not just on the harm, but also on the effect of the defendant's intentional activities on a State, for example, on where the defendant intentionally distributed his goods online. So far, it is unclear whether in the EC an online seller will be taken to have 'distributed' his site wherever it can be accessed or only in those States to which it is specifically targeted.

Were the judges in *Gutnick* correct in arguing that things are not as bad as they seem, that, at least in respect of defamation, online publishers can easily anticipate the location of any potential harm – by reference to the person written about – and then take measures to comply with that particular legal regime? As attractive and simple as it sounds, this argument is flawed in principle for a number of reasons. First, to somehow suggest that only those online publishers who cause harm in a State will be exposed to its laws, is misleading and does not at all reduce their regulatory burden. As long as one complies (knowingly or unknowingly) with a law, one may very well get the impression that that law does not exist or that it does not apply to one's

[91] Art. 5 of *Amended Proposal for a European Parliament and Council Regulation on the Law Applicable to Non-Contractual Obligations (Rome II)*, COM(2006) 83 final. Note that defamation is currently excluded for lack of agreement: see Amendment 57 and Art. 1(2)(h).

[92] *Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations (Rome II)*, COM(2003) 427 final, 11f (explaining the background to Art. 5).

[93] *Shevill* v. *Presse Alliance SA*, Case C-68/93 [1995] ECR I-415, para. 30.

actions.[94] But, if a law applies, it is there during compliance and during non-compliance (although hopefully more overtly in the latter case). Causing 'harm' in a State never triggers the application of a State's law, but the occurrence of the 'harm' presupposes its prior application. To say that 'harm' has been caused is simply another way of saying that the law (which applied) has been breached. The question is what attracted the application of the law in the first place. By definition, it cannot be the 'harm' itself. Generally, it would be the defendant's activities on the State's territory. In the defamation context, that activity would be publishing on the territory. And when this activity on the particular territory is carried on knowingly, then it seems reasonable to hold that the application of the local laws was foreseeable.

Secondly, relying on the foreseeability of harm is also intrinsically flawed for another reason. It is based on the idea that there is such a thing as objective, universal harm which should be obvious to anyone anywhere. Yet this is not the case. 'Harm' is a legal construction, defined by, and dependent on, the particular legal system and legal culture. What is 'harm' in one legal system may not be recognised as 'harm' in another (except for some universally recognised 'harm', such as bodily harm). In terms of foreseeability, this means that what appears to be blatantly obvious 'harm' in one legal culture is not at all obvious from the perspective of an outsider. So, while 'damage to one's reputation' seems rather obvious, it is less so when one considers the position under Chinese law, where it is possible to damage the reputation of the dead.[95] Would an English journalist writing a historical account of Mao Zedong even pause to consider if any 'harm' could be caused by it to anyone? Would a US publisher, particularly a small one, expect that not all States share the 'obvious' distinction between 'public figures' and 'private figures' made under US defamation law? And this is still only within the boundaries of defamatory harm. Saying that local defamatory 'harm' can easily be foreseen by a foreigner has a distinct whiff of parochialism about it.[96]

[94] Generally, both from a regulator's and a publisher's perspective, knowing compliance is desirable and that entails taking proactive steps towards ascertaining all relevant law before any potential harm is caused.

[95] See e.g. Joy Jacobson, 'Of Love and Defamation in China' (2003) *Poets & Writers Magazine*, www.pw.org.

[96] Note the argument that the publisher ought to foresee the foreign law by reference to the potential harm caused abroad is also circular. As the 'harm' is the 'harm under foreign law' the publisher can only foresee that harm if he foresees the application of the foreign law in the first place.

Thirdly, focusing on the foreseeability of harm also suggests that the publisher foresees the possibility that damage to reputation may be caused by its article in the first place. This may very well be the case.[97] However, under traditional common law defamation law, the defamation itself need not be intentional or even negligent. A publisher may be liable for defamation even though it had no idea that the article was false or defamatory in any way. Consequently, it makes no sense to argue that such a publisher could have anticipated foreign defamation law on the basis of the potential harm – if it foresaw none whatsoever.[98]

For these reasons, it is submitted that the High Court was wrong when it stated that defamation was different from 'cases, like trespass or negligence, where some quality of the defendant's conduct is critical'.[99] And that conduct cannot but also be critical in defamation to satisfy the foreseeability requirement. In defamation, that critical conduct is publishing. What must be intentional under traditional defamation law in England or Australia is the publication itself.[100] Significantly, 'publication' at common law has never been exclusively concerned just with the final *fact* of publication but also with the initial *act* of publication, that is, whether or not the defendant intended the publication, or where the publication was at least reasonably foreseeable. For example, it has been held that there is no publication in law, even though there is a publication in fact, where a writer locks a disparaging letter in a drawer and a thief finds the letter and publishes it.[101] There is no publication by the

[97] Particularly where the 'publisher' is the author or editor, but less likely so where the publisher is further removed from the initial source, as, for example. a distributor of any kind.

[98] In the US, personal jurisdiction may be based on intentionally causing harm in the forum: *Calder* v. *Jones*, 465 US 783 (1984). This is applicable to intentional torts, including, under US law, defamation which requires *N* depending on the 'public' or 'private' status of the defamed plaintiff *N* that the publisher knew the statement was false or was at least reckless or negligent as to its falsity and thus knew of its defamatory potential. In other words, foreseeing harm or injury is an ingredient of the US defamation action. *New York Times Co.* v. *Sullivan*, 376 US 254 (1964); *Gertz* v. *Robert Welch Inc.*, 418 US 323 (1974).

[99] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 43, distinguishing defamation from cases of misrepresentation, e.g. *Voth* v. *Manildra Flour Mills* (1990) 171 CLR 538, where it held that the focus should be on the substance of the defendant's act and not its consequences. See also *Distillers Co. (Biochemicals) Ltd* v. *Thompson* [1971] AC 458 (PC).

[100] See above n. 70.

[101] *Pullman* v. *Walter Hill & Co. Ltd* [1891] 1 QB 524, 527; see also *Huth* v. *Huth* [1915] 3 KB 32; *Powell* v. *Gelston* [1916] 2 KB 615.

writer because he did not intend the publication. By the same token, a newspaper published in the UK is not published in Japan, merely because a Japanese person buys the paper in the UK and takes it back to Japan and reads it there.[102] The original distributor never intended publication in Japan; that publication is entirely fortuitous. It is precisely this intention to publish here, but not there, which means that to a publisher the laws of one State are foreseeable and the laws of another are not. In short, if a person intentionally publishes in a certain State, then it seems entirely reasonable to expect the person to foresee and comply with the laws of that State.

It is of course a matter of considerable debate *where* an online publisher ought to be taken to have intended to publish the material on its site. The above courts have all expressly or implicitly endorsed the 'worldwide intention' proposition: a publisher of a freely accessible site must be taken to have intended to publish the material on that site everywhere. That is one possible stance. But, if one adopts that position, it is theoretically highly unsatisfactory to argue that the foreseeability of the local harm softens its ramifications. First, 'harm' is a legal construction dependent on the particular legal culture and not easily foreseeable from the outside. Secondly, when the 'harm' has not been intended but is still actionable, it is also difficult to base the foreseeability of foreign law on that unforeseen harm. Another possible stance on 'objective intention' is to focus on specifically targeted destinations.

Foreseeability of specifically targeted destinations[103]

An alternative to the 'worldwide intention' proposition is the notion that most websites specifically target only one State or a limited number of States, and that intention is ascertainable objectively from the general context of the site. Following this approach, actual access is not sufficient to establish competence, but must be accompanied by a clear

[102] *Kroch* v. *Rossell* [1937] 1 All ER 725, where very few copies of a French and a Belgian newspaper, mainly distributed in France and Belgium, had been distributed in England through a distribution company, which bought and resold the magazine. The English court refused to exercise adjudicative jurisdiction, as the tort committed in the jurisdiction was not a real and substantial one. Noteworthy here, although not relied upon by the court, was that the foreign distribution would have been entirely fortuitous from the perspective of the initial publishers; it was only within the control and knowledge of the distribution company. For the requirement of a purposeful publication, as opposed to a fortuitous one, under German law, see Hestermeyer, above n. 2, 282.

[103] Same as the 'reasonable' effects test, discussed in Chapter 3, Section 4.B, above.

intention to direct the site at the particular State. An essentially local publication, such as a local newspaper, does not turn into a worldwide publication simply and automatically because it is made available on the Internet, even if it is occasionally accessed from foreign locations. This approach has been adopted in the US, in the context of adjudicative jurisdiction in online defamation disputes.[104]

An early defamation case which recognised the specific territorial focus of sites is *Blumenthal* v. *Drudge*,[105] in which the District of Columbia Court held that it had jurisdiction over the Californian defendant Drudge in respect of a claim involving the Drudge Report, published on the Internet from the defendant's computer located in California and allegedly defamatory of the plaintiffs in the District of Columbia. While the defendant sent emails with the report to subscribers of the site, of which only a fraction came from California, he in fact had no way of identifying their location. Thus he could not *prima facie* be said to have intentionally published the report in the District of Columbia.[106] Had he, like Dow Jones in *Gutnick*,[107] known the location of his readers, then the targeting issue would been more straightforward. Nevertheless, the court found that the Californian site targeted the District of Columbia, as 'Drudge specifically targets readers in the District of Columbia by virtue of the subjects he covers'.[108] The subject-matter of the site defined and territorially delimited the readership of the site.

More recently, in *Young* v. *New Haven Advocate*,[109] two Connecticut newspapers were alleged to have defamed the plaintiff in Virginia by virtue solely of their online editions. In a thoughtful and persuasive

[104] In the US, adjudicative and subject-matter jurisdiction are not as obviously linked, but, if jurisdiction is based on specific personal jurisdiction, the tort is invariably generally committed in the forum. See also above n. 3.

[105] 992 F Supp 44 (1998). [106] *Blumenthal* v. *Drudge*, 992 F Supp 44, 54 (1998).

[107] Dow Jones, by accepting subscriptions from Australian residents, knowing they were Australian, targeted Australians with its site. While Australia may not have been the primary target, which was the US market, it was certainly a secondary target. Kirby J acknowledges this when he questions whether a 'targeting' approach would, if applied, also lead to a finding of a publication in Victoria. *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 131.

[108] *Blumenthal* v. *Drudge*, 992 F Supp 44, 57 (1998).

[109] 315 F 3d 256 (2002), reversing 187 F Supp 2d 498 (WD Va 2001), where the lower court had taken the *Gutnick* approach: '[T]he defendants argue that it would be unfair to subject them to worldwide jurisdiction simply because they placed information on the Internet . . . Again, this court disagrees.'

judgment, the Fourth Circuit court held that the newspapers need not defend proceedings in Virginia 'because they did not manifest an intent to aim their websites or the posted articles at a Virginian audience'.[110] The electronic activity was not directed at the State with 'the manifested intent of engaging in business *or other interactions* within the State'.[111] The papers had not conceptually 'entered' the State with their sites. They were local sites aimed at a local audience only:

> The overall content of both websites is decidedly local, and neither newspaper's website contains advertisements aimed at a Virginian audience. For example, the website that distributes the Courant . . . provides access to local . . . weather and traffic information and links to websites for the University of Connecticut and Connecticut state government . . . Connecticut, not Virginia, was the focal point of the articles.[112]

Most interestingly, the court rejected (exactly what the High Court of Australia endorsed) the notion that the online publishers could be expected to defend litigation in Virginia because they posted potentially injurious matters on the Internet knowing full well that the plaintiff resided and worked in Virginia.[113] The court held that the foreseeability of foreign harm is not enough to expose the defendant to the foreign court processes. They reiterated what seems an entirely appropriate proposition: 'Although the place that the plaintiff feels the alleged injury is plainly relevant to the . . . inquiry, it must ultimately be accompanied by the defendant's own . . . contacts with the state if jurisdiction is to be upheld.'[114] In the final result, the defendant's activities of course outweighed the location of the harm. This is consistent with the above argument, that the competence inquiry (in any legal context, including defamation) should not hinge on where the harm was knowingly inflicted but rather on where the material on the site was knowingly published, i.e. at whom it was directed.

If material on a site is not – as in *Gutnick* or the other English cases – taken to be knowingly published everywhere, the inquiry as to where in particular the site was targeted will often (but not always) yield the same location where the defamatory harm was suffered. This is simply because generally articles about a person are directed at those readers who

[110] *Young* v. *New Haven Advocate*, 315 F 3d 256, 258f (4th Cir. 2002).
[111] *Ibid.* (emphasis added). [112] *Ibid*., 263. [113] *Ibid*., 262.
[114] *Ibid*., 262, citing *ESAB Group Inc.* v. *Centricut Inc*., 126 F 3d 617, 626 (4th Cir. 1997); following *ALS Scan Inc*. v. *Digital Service Consultants Inc*., 293 F 3d 707, 714 (4th Cir. 2002).

know, or live in the same community as, that person. However, as a matter of principle, and occasionally as a matter of substantive justice, it is vital to frame the inquiry correctly and to examine the publication itself rather than the 'harm'. The harm, but not the publication, may be unintentional and thus its location fortuitous to the publisher.

The court also showed how a site's territorial focus can be ascertained in the case of non-interactive, non-commercial websites: simply examine the general thrust and content of the site. Just because a site is passive and non-commercial does not mean that it is not subject to the laws of any State; it is subject to the laws of those States which it objectively targets in light of all the circumstances. This is exactly the same broad notion that underlies the *Zippo* test or the EU's 'directing' test for consumer contracts: no pain no gain. Here, the gain is simply attracting readers from a certain State.[115] It is the moderate country-of-destination approach, applied to the particular context of online defamation.

This targeting approach has been applied to torts outside the US. Most interestingly, the High Court of Australia itself endorsed it in *Voth* v. *Manildra Flour Mills* in respect of negligent misrepresentations:

> If a statement is directed from one place to another place where it is known or even anticipated that it will be received by the plaintiff, there is no difficulty in saying that the statement was, in substance, made at the place to which it was directed . . . And the same would seem to be true if the statement is directed to a place from where it ought reasonably to be expected that it will be brought to the attention of the plaintiff.[116]

Similarly, in the Scottish trademark case of *Bonnier Media Ltd* v. *Greg Lloyd Smith*, Lord Young adopted a targeting approach, noting that he saw no reason 'why similar principles should not be applied to delicts such as defamation, or indeed negligence'.[117] He summarised it perfectly:

> the person who sets up the website can be regarded as potentially committing a delict in any country where the website can be seen, in other words in any country in the world. It does not follow that he actually

[115] The no-gain-no-pain maxim has been applied to the outright destination approach: the gain would simply be the worldwide audience acquired by virtue of going online, which is fictional in respect of most localised websites.

[116] *Voth* v. *Manildra Flour Mills* (1990) 171 CLR 538, para. 63.

[117] *Bonnier Media Ltd* v. *Greg Lloyd Smith and Kestrel Trading Corporation* (Court of Session, Scotland, 1 July 2002), para. 18, www.scotcourts.gov.uk/opinionsv/dru2606.html.

> commits a delict in every country in the world, however. It is obvious that the overwhelming majority of websites will be of no interest whatsoever in more than a single country or small group of countries. In my opinion a website should not be regarded as having delictual consequences in any country where it is unlikely to be of significant interest . . . In determining whether the impact of a website is insignificant, it is appropriate in my opinion to look both at the content of the website itself and at the commercial or other context in which the website operates.[118]

E. Two destination principles: their flaws and merits

This targeting approach is not flawless. It lacks certainty, as discussed in Chapter 3. Even in *Young* it could have been argued that the newspaper which had accepted eight subscriptions from Virginia[119] also targeted Virginia provided the locations of subscribers were known. Virginia might not have been the primary target, but it might have been one of many secondary targets. The difficult question is how great the proportion of the overall readership must be before a State can be considered a target of the site? And this question is not amenable to an easy and certain answer. However, the main disadvantage which probably explains why many courts have not gone for the targeting approach (and even less so for the country-of-origin approach) is that it requires States to forego competence even though the site had some effect, albeit minor, on the territory. Non-targeted States may often be marginally affected by the site, but the whole point of the targeting approach is to let only those significantly affected regulate it. Sporadic and isolated hits on a site from any country should simply be ignored for competence purposes. That seems unacceptable from the perspective of most States as it would mean that more lenient foreign legal standards can compromise, however marginally, home-grown legal policies. This shines through Hedigan J's comments in *Gutnick*:

> The . . . argument that it would be unfair for the publisher to have to litigate in the multitude of jurisdictions in which its statements are downloaded and read, must be balanced against the world-wide inconvenience caused to litigants . . . who would at enormous expense and inconvenience have to embark upon the formidable task of suing in the

[118] *Ibid*., para. 19 (emphasis added); same approach as in *Euromarket Designs Inc*. v. *Peters* [2000] ETMR 1025.

[119] *Young* v. *New Haven Advocate*, 315 F 3d 256, 260 (4th Cir. 2002).

> USA . . . where the libel laws are . . . tilted in favour of defendants, or . . . in favour of the constitutional free speech concepts and rights developed in the USA which originated in the liberal construction by the courts of the First Amendment.[120]

In the High Court of Australia, Callinan J defended the approach adopted on the basis that anything else would create 'an American legal hegemony in relation to Internet publications'.[121] And, of course, he had a point because the more lenient speech standards would to some limited extent infiltrate countries with stricter standards on any approach other than the outright country-of-destination approach. But by insisting on competence over all online activity States shoot themselves in the foot. And this brings us to the substantial advantages of the moderate country-of-destination approach.

First, it reduces the regulatory burden of online content providers to a more realistic level; they need only comply with the laws of the States which they specifically and substantially target and not the laws of all States. The importance of this cannot be overstated. To create any order in cyberspace, the first step must be realistic legal expectations. Currently, many people still believe that the Internet is not or is only marginally regulated by States. In truth, States have made broad regulatory claims over sites (often without any means of enforcing these claims) across the legal spectrum, so much so that most sites attract a vast array of legal regimes – far too great for most online publishers to comply with. This means that legal non-compliance[122] cannot but be the default position in cyberspace – a position hardly conducive to law and order. A wider endorsement of the targeting approach would be a step in the right direction of aligning legal expectations by States with the legal capacity of most online actors.

Secondly, despite its lack of certainty, the targeting approach still accommodates foreseeability and control. Online actors, just like the courts, can foresee possible legal exposure by examining the general thrust and content of their sites, and can limit their legal exposure by changing that general thrust and content, by making the site interesting

[120] *Gutnick* v. *Dow Jones & Co. Inc.* [2001] VSC 305, para. 73.

[121] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 200.

[122] This may often take the form of accidental 'compliance'. In other words, a site may not breach a law not because the operator consciously complied with it, but rather because his conduct happened to be in conformity with the law. Despite not breaching the law, the online actor cannot be said to comply with it as compliance entails knowing the law and consciously acting in accordance with it.

for visitors from one State but not another. And, as isolated, sporadic hits are ignored for legal purposes, freely accessible sites are legally accommodated: they do not need to be transformed into sites with access restrictions to gain control over their visitors and thus their legal exposure. This would seem to be highly desirable to protect the openness and accessibility of the Internet as a whole.

Thirdly, the targeting approach allows States to make regulatory claims (i.e. to apply their laws and court procedures) in respect of those foreign activities which have a real effect on their territory. Last but not least, on a theoretical level the moderate country-of-destination approach protects the integrity of any transnational regime allocating regulatory competence. These regimes are premised on the assumption that not all States should regulate all activities: they should *share* competence amongst themselves, based on the *relative* strengths of the nexus between the activity and the State.

The table summarises the flaws and merits of the two destination principles.

Outright country-of-destination approach	Moderate country-of-destination approach
Legal exposure based on online accessibility of the site in a State	Legal exposure based on directing online activities towards a State
EXAMPLES	
Gutnick, *Harrods*, *King* *Yahoo*, *Töben*, *Perrin*	Art. 15(1)(c) of the EC Jurisdiction Regulation US jurisprudence on personal jurisdiction: *Zippo* targeting test, the *Young* effects doctrine
ADVANTAGES	
In principle, States retain absolute control over their territory (regulate sites with an effect, even if minor, on their territory, i.e. all accessible websites) – local policies, businesses, consumers protected	In principle, States retain control over their territory (regulate sites with a significant effect on their territory, i.e. websites which are frequently accessed) – local policies and consumers largely protected
Simple (easy foreseeability of foreign legal regimes, namely all)	Fewer concurrent assertions of competence; more realistic regulatory burden for online publishers

Table (*cont.*)

Outright country-of-destination approach	Moderate country-of-destination approach
DISADVANTAGES	
Innumerable concurrent assertions of competence; significant overregulation of online publishers (non-compliance is the default option)	States lose some control over their territory (activity which has a minor effect is not regulated)
Inconsistent with the idea of sharing competence between States, which underlies all competence regimes	Lack of certainty and predictability; targeting may lead to varying conclusions
Often not enforceable	Often not enforceable

3. Foreseeability of foreign criminal law

A. Common rules but multiple interpretations

The criminal jurisdiction of States is delimited by public international law. Thus in principle there is only one set of rules, in contrast to the many sets of private international laws – making exposure to foreign criminal law in principle more easily foreseeable. The reality is not as clear cut. First, while the territoriality principle itself, the primary basis of criminal jurisdiction, is unchallenged, its boundary areas (for example, the effects doctrine) are controversial;[123] and many online cases fall into grey areas. Secondly, the precise limits of criminal jurisdiction are invariably determined by national courts which make decisions as to the width of their competence, often preoccupied by local policy, without reference or regard to international law[124] or the need for internationally harmonised rules.[125] Unless those decisions seriously affect the national interests of other States, protests by them against too wide an

[123] See Chapter 3, section 4, above. See also Rosalyn Higgins, 'The Legal Bases of Jurisdiction', in Cecil J. Olmstead (ed.), *Extraterritorial Application of Laws and Responses Thereto* (Oxford: ECS Publishing Ltd, 1984), 3, 5ff.

[124] A typical example is the recent Australian decision of *Lipohar* v. *R* (1999) 168 ALR 8, 48, where the judges, referring *obiter* to the issue of international jurisdiction, at most acknowledged international comity, as opposed to legal limits set by international law.

[125] Sir Robert Jennings and Sir Arthur Watts (eds.), *Oppenheim's International Law* (9th edn, London: Longman, 1992), Vol. 1, 45, noting that 'in many states the courts have to

assumption of regulatory control are rare.[126] It means that the existence of an international jurisdictional regime does not pre-empt inconsistencies of jurisdictional assertions or the national fragmentation of principles. Assertions of criminal jurisdiction are unlikely to be more easily foreseeable than legal exposure in the private context simply by virtue of 'harmonisation' at international level.

Furthermore, public international law is designed to maintain an orderly system between States, allowing them to promote their national interest and welfare without interference from other States.[127] The interests of individuals are of secondary importance and subordinate to those of States. This is, for example, reflected in the rule that individuals cannot contract in or out of the public ordering of a State, comparable to private law. In respect of US anti-trust law, one commentator said '[v]oluntary submission clauses would not make US jurisdiction more palatable. Foreign recipients of US goods or technologies admittedly often "agree to comply" with US export control regulations. But private companies cannot, as a rule, restrict the jurisdiction of their sovereign state by a private contractual obligation.'[128] All public law is of a mandatory character and

apply their national laws irrespective of their compatibility with international law'. Karl M. Meessen, 'International Law Limitations on State Jurisdiction', in Cecil H. J. Olmstead (ed.), *Extraterritorial Application of Laws and Responses Thereto* (Oxford: ECS Publishing Ltd, 1984), 38, 39. Note also the much criticised *dictum* in *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No. 10, 19: 'far from laying down a general prohibition to the effect that states may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion which is only limited in certain cases by prohibitive rules; as regards other cases, every state remains free to adopt the principles which it regards as best and most suitable.'

126 Michael Akehurst, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145, 169 and 187. Note also Comment 'd' to §402 of the US Restatement (Third) of Foreign Relations Law (1986), stating that the controversy over the effects doctrine has been generally limited to jurisdictional assertion based on economic effects, particularly through competition laws.

127 Bernard H. Oxman, 'Jurisdiction of States', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 277, 278.

128 Luzius Wildhaber, 'The Continental Experience', in Cecil H. J. Olmstead (ed.), *Extraterritorial Application of Laws and Responses Thereto* (Oxford: ECS Publishing Ltd, 1984), 63, 66. Note that companies not infrequently enter into agreements with States themselves under which they may enjoy immunity, from certain laws in return for inward investment. In such situations, the State is a party to the contracting out of legal obligations. Generally, Philip J. McConnaughay, 'Reviving the "Public Law Taboo" in the International Conflicts of Law' (1999) 35 *Stanford Journal of International Law* 255, 280, where the author refers to recent US cases where private parties to international transactions appear to have been allowed to opt out contractually of otherwise applicable US public law. See also Australian Law Reform

can never, in terms of foreseeability, benefit from party autonomy. So the criminal jurisdiction regime can hardly be said to have a head start when it comes to foreseeability of legal exposure.

B. Foreseeability and the territoriality principle

Does the territoriality principle incorporate foreseeability of legal exposure as a prerequisite for its application? A critic of Johnson and Post's argument about the absence of noticeable borders in cyberspace argued that the 'argument wrongly imports a notice requirement for prescriptive jurisdiction . . . But, international law does not in fact require a state to satisfy a reasonableness standard in exercising prescriptive jurisdiction.'[129] But does international law indeed condone States acting in disregard of the rule of law by subjecting individuals to their laws in situations when they could not have known about them? Such sentiments would seem to be entirely irreconcilable with the notion of human dignity reflected in universally recognised human rights.

One reason why the territoriality principle developed as the main organising principle for allocating regulatory control is that territory or physical distance was, and is, albeit to a lesser extent, determinative of our behaviour, with whom we interact and upon whom our actions have an effect.[130] When physicality or location is determinative of, and delimits,

Commission, *Choice of Law*, Report No. 58 (1992), para. 8.27, www.austlii.edu.au/au/other/alrc/publications/reports/58/, In *R* v. *Harden* [1963] 1 QB 8, the court refused to exercise jurisdiction in a criminal case because the accused had agreed with his victims that certain documents were deemed to be received by the accused in New Jersey when they were received by the New Jersey post office; discussed in Matthew Goode, 'The Tortured Tale of Criminal Jurisdiction' (1997) 21 *Melbourne University Law Review* 411, 418f. This decision, which has frequently been criticised, appears contrary to established practice.

[129] Sanjay S. Mody, 'National Cyberspace Regulation: Unbundling the Concept of Jurisdiction' (2001) 37 *Stanford Journal of International Law* 365, para. II.B. But is reasonableness the same as notice? Similar views are expressed in Karl M. Meessen, 'International Law Limitations on State Jurisdiction', in Cecil J. H. Olmstead (ed.), *Extraterritorial Application of Laws and Responses Thereto* (Oxford: ECS Publishing Ltd, 1984), 38, 39: 'as regards state jurisdiction, those factors listed in *Timberlane* and *Mannington Mills* that are exclusively related to the protection of the individual . . . are rather unlikely to form part of international law proper.'

[130] Santiago Torres Bernardez, 'Territorial Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 487, 487f: 'it enables the integration of the State's human constituents to take place through its attachment to the soil . . . and provides a solid basis for the powers of control and coercion . . . [but] it must be admitted that in recent decades the material function of territory has . . . been

human interactivity, making it a basis for regulatory competence makes sense because of its simplicity and transparency for all concerned: 'In practice . . . the [territorial] rule was adopted because it was thought that it would be easy to apply and would produce certainty of result.'[131] The emergence of the territoriality principle as the main organising principle for allocating regulatory competence cannot but have been linked to the high degree of foreseeability of legal consequences which it could produce in a human environment constrained by physical distance. Yet, this does not mean that the foreseeability of legal consequences is also incorporated within the territoriality doctrine as a prerequisite for legal exposure.

When the foreseeability of legal exposure is clearly present (as when the relevant action or actors are located within one territory only), then it need not be decided if it is in fact a pre-requisite for legal exposure. Such a decision is only required when foreseeability is in doubt, as was the case, for example, in respect of US antitrust law being applied to anti-competitive practices occurring outside its territory.[132] The law was applied to foreign actors who never entered US legal space, never crossed its borders, never passed those signposts alerting them to the start of new legal space. The only things to transit those borders were the economic effects of their actions. In terms of foreseeability, this was problematic, especially because corporate activities frequently have economic effects of varying intensity in a number of States,[133] making it difficult to predict which States have a right to regulate and which do not. Yet, whatever criticism one may mount against the effects doctrine, foreseeability was tackled from the outset. In the seminal *Alcoa* case, the judges held that jurisdiction could only be asserted over foreign activities which were subjectively intended to affect the US and did actually affect the US.[134] Given the difficulty of proving anyone's subjective intention, '[t]he requirement of subjective intention to affect American trade or commerce was soon replaced by the objective tests of foreseeability of

affected by the impact of such new phenomena as fast communications, sophisticated weaponry and integrated economic regions.'

[131] Goode, above n. 128, 415.

[132] In the seminal case in this area, *US* v. *Aluminium Company of America* (the Alcoa case), 148 F 2d 416, 443 (1945), this expansion of competence was justified by the following, later much disputed, statement: '[I]t is settled law . . . that any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends.'

[133] Akehurst, above n. 126, 195. A typical recent example is the collapse of Enron plc.

[134] The Alcoa case (*US* v. *Aluminium Company of America*), 148 F 2d 416, 444 (1945).

that effect'.[135] More precisely, US law would apply when 'foreign transactions have a substantial and foreseeable effect on US commerce'.[136] When the effect of someone's activity on a State is both substantial and foreseeable, it is foreseeable (and must be foreseeable to the actor in question) that that State has a legitimate interest in regulating that activity. Thus its laws are foreseeable. The 'substantial and foreseeable effect' requirement appears to have survived all later US developments (including the rise and fall of the 'balancing test'[137]), with the current position permitting jurisdiction over foreign activity only if it was intended to, and did, produce substantial effects on US territory.[138] The following examines how foreseeability has been dealt with in regulating online conduct through public law.

C. *Foreseeability of all destinations*

The crux of the problem in respect of criminal jurisdiction over online activity is the same as with jurisdiction in private cases: online publishers, especially of freely accessible sites – the bread and butter of the Internet – often do not know the location of those who access or might access their sites, or, even if they do, it may not be practicable to exclude certain users without transforming the site significantly. A classic example would be the freely available preview site (to a subscription pornography site) in respect of which Perrin was convicted in the UK for an obscenity offence.[139] Online publishers have argued that they do not necessarily know which State they 'enter' and thus cannot foresee the law to which they may be exposed.[140] Have States been sensitive to this

[135] A. V. Lowe (ed.), *Extraterritorial Jurisdiction – An Annotated Collection of Legal Materials* (Cambridge: Grotius Publications Ltd, 1983), 3.

[136] *Ibid.*

[137] Introduced by *Timberlane Lumber Co.* v. *Bank of America*, 549 F 2d 597, 614–15 (1976), which required the court in deciding jurisdiction also to take into account a number of factors, including 'the extent to which there is explicit purpose to harm or affect American commerce, [and] the foreseeability of such effect'; followed in *Mannington Mills* v. *Congoleum Corp.*, 595 F 2d 1287, 1294ff (1979); see §§402 (1)(c) and 403(2)(a) and (d) of the US Restatement (Third) of Foreign Relations Law (1986). The balancing test was rejected in *Hartford Fire Insurance Co.* v. *California*, 509 US 764 (1993).

[138] American Bar Association (ABA), 'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, www.tlaw.edu/cyberlaw/docs/drafts/draft.rtf, 82.

[139] *R* v. *Perrin* [2002] EWCA Crim 747.

[140] Perrin relied on interpretation of the 'rule of law' by the European Court of Human Rights in *Sunday Times* v. *UK (No. 1)* (1979) 2 EHRR 245, para. 49: '[T]he following are

argument? The answer is both yes and no. Yes, courts, despite endorsing the country-of-destination approach, have, often expressly, taken foreseeability into account. Yet, this express concern has not been translated into a serious engagement with the overall legal burden of online publishers, and has invariably led to the implicit conclusion that going online makes worldwide regulation foreseeable.

For example, in the *Yahoo* case, the French court was not oblivious to the notion of foreseeability, despite the fact that, in the initial judgment in May 2000, Justice Gomez justified France's competence on the basis that Yahoo! Inc, by permitting the online visualisation in France of the objects in question, 'has committed a wrong on the Territory of France, a wrong, the *unintentional nature* of which is apparent'.[141] This argument was somewhat retracted in the November judgment:

> while it may be accurate that the site 'Yahoo Auctions' in general is intended principally to internauts based in the United States given the nature of the objects put on sale, the methods of payment provided, the terms of delivery, the language and the currency used, *the same is not true of the sites auctioning objects representing symbols of the Nazi ideology which might interest and are accessible to any person who wishes to go to them, including French people*.[142]

The court imputed to Yahoo! Inc. an intention to offer the Nazi objects to the world at large, including France, based on the nature of the objects, which may be of interest anywhere. This intention, in the court's mind, was further evidenced by the fact that Yahoo! Inc. provided online advertising which was sensitive to the location of surfers, with surfers accessing the auction site from France being sent advertising banners in French.[143] So, far from saying that Yahoo! Inc.'s intentions were

two of the requirements that flow from the expression 'prescribed by law'. Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable.'

[141] *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000) (emphasis added); affirmed in *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000), www.foruminternet.org/actualites/lire.phtml?id=273/.

[142] *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000) (emphasis added).

[143] *Ibid.*

irrelevant, Justice Gomez held that anyone offering Nazi memorabilia can be presumed to realise that it is of interest worldwide and thus must be taken to have intended worldwide distribution.[144] Worldwide legal exposure was foreseeable. Similarly, in the *Töben* judgment, the German court justified the assumption of jurisdiction by arguing not only that a constituent element of the crime had occurred in Germany[145] but also that Töben had intended this: by putting the Holocaust denials on the Internet, he intended to publish his assertion worldwide and thus also in Germany. The court did note that, given the content of the site, it was objectively intended in particular for a German audience.[146]

Interestingly, in both cases the court focused on the content of the particular site to determine the site's objective territorial target. However, the difference to the *Young* approach is that, at least in *Yahoo*, the focus was very narrowly on the particular matter which actually caused the harm, rather than on the general territorial focus of Yahoo! Inc.'s auction site or the entire yahoo.com. So Justice Gomez really argued very much along the lines of the *Gutnick* court: look at the particular person written about, or hear the particular thing offered on your site, which caused the 'harm' in our State and you, the online publisher, could have known that that 'harm' would occur here. So 'harm' is treated, just like 'harm' in defamation, as if it were something objectively existent, disconnected from any particular legal system, which should by itself alert the publisher to the application of the law. But, as argued above, harm is what each legal system defines as 'harm', often very differently. So, again, the courts took a parochial view on foreign online activity to support the foreseeability of domestic rules.

A seemingly more moderate country-of-destination approach appears to have been adopted by US courts. They seem to follow their antitrust precedents, requiring as a foundation for criminal jurisdiction that the foreign conduct was intended to, and did, produce actual effects

[144] *R* v. *Timothy K and Yahoo Inc.* (Tribunal de Grande Instance de Paris, 26 February 2002, No. 0104305259), www.foruminternet.org/actualites/lire.phtml?id=273/, where the court reinforced the importance of intention. Although the advertising was a constituent element, and indeed essential characteristic, of the relevant crime, 'the factual circumstances of the advertising must reveal the intention of the publication . . . there is no reprehensible advertising if it results from independent and posterior circumstances foreign to the intention of its author'.

[145] In this case, this was the real capability of the online material to disturb the public peace in Germany: *Töben* (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624, 626f.

[146] *Ibid*., 627.

in the territory. For example, in the early consumer protection case of *State of Minnesota* v. *Granite Gate Resorts Inc.* dealing with deceptive trade practices, the Minnesota court assumed adjudicative jurisdiction over the foreign defendant on the basis of 'the computer hits on Defendants' Web sites . . . along with the fact that the Court has determined that WagerNet's mailing list includes Minnesota residents'.[147] Furthermore, its advertisement on an American commercial site suggested that the defendant intended to reach an American market.[148] All in all, the defendants had 'made a direct marketing campaign to the State of Minnesota. Therefore, it is not unforeseen nor unreasonable to Defendants to be required to come to Minnesota to defend themselves.'[149] A similar approach was taken in *People* v. *World Interactive Gaming Corp.*,[150] where the court held that the site operators had targeted the US and thus also New Yorkers:

> WIGC . . . [is] doing business in New York . . . [It] engaged in an advertising campaign *all over the country* to induce people to visit their website and gamble. *Knowing* that these ads were reaching thousands of New Yorkers, respondents made no attempt to exclude *identifiable* New Yorkers from the propaganda. Phone logs from respondents' toll-free number (available to casino visitors on the GCC website) indicate that respondents had received phone calls from New Yorkers.[151]

Of course, this reasoning is not conclusive as to the position the court would have adopted if the defendant had not directed its activities so clearly primarily at the US. What would the court have decided if the US had merely been a secondary target with European States being the primary target? Given the economic power of the US and its

[147] *State of Minnesota* v. *Granite Gate Resorts Inc.*, 558 NW 2d 715, 720 (1997), affirming *State of Minnesota* v. *Granite Gate Resorts Inc.*, WL 767431 (Minn. 2d Dist. Court, 1996). Although US courts largely apply the same principles to public prosecutions as those governing personal jurisdiction in private cases, the court in *State of Minnesota* v. *Granite Gate Resorts Inc.*, WL 767431 (Minn. 2d Dist. 1996), 10, said: 'Minnesota through the Attorney General seeks to regulate solicitation that comes to its state via phone lines hooked up for Internet users. The Courts do not view the contacts the same as what is necessary for a private litigant to pursue a case as compared to the situation in which the state seeks to regulate solicitations within its borders.' Most States would require as a precondition for a prosecution the actual presence of the offender in the territory, not merely 'minimum contacts'.

[148] *State of Minnesota* v. *Granite Gate Resorts Inc.*, 558 NW 2d 715, 720 (1997).

[149] *State of Minnesota* v. *Granite Gate Resorts Inc.*, WL 767431 (Minn. 2d Dist. Court 1996), 7.

[150] 714 NYS 2d 844 (1999). [151] *Ibid.*, 849 (emphasis added).

technological sophistication, it is an attractive market for online businesses around the globe. So being a secondary target is not a question US courts have to consider often; generally they can comfortably adopt a seemingly more moderate legal stance on competence, as more often than not adopting that stance justifies their competence. Isolated examples suggest that, if the need arises, even the US will not be quite as generous on the competence issues.[152]

Certainly, in criminal law, even more so than in private law, all States are deeply concerned about foregoing regulatory competence when that would undermine local policies or, as will be shown in the next chapter, local economic interests. For now, the sentiments expressed by the court in *People* v. *World Interactive Gaming Corp.*[153] accurately reflect the concern all States share about foreign online activity which is illegal at home:

> Wide range implications would arise if this Court adopted respondents' argument that activities or transactions which may be targeted at New York residents are beyond the state's jurisdiction. Not only would such an approach severely undermine this state's deep-rooted policy against unauthorized gambling, it also would immunize from liability anyone who engages in any activity over the Internet which is otherwise illegal in this state.[154]

D. 'Reasonable foreseeability': some conclusions

What is 'reasonably foreseeable' is not something objectively ascertainable by reference to human or corporate capacity to absorb legal regimes. If this were the case, it would yield the same conclusion regardless of the particular legal context or the legal regime. But clearly a foreign legal order not reasonably foreseeable in one context may nevertheless be considered foreseeable in another. 'Reasonable

[152] One example taken from the private context is the trademark case of *Cable News Network LP* v. *CNNews.com*, 177 F Supp 2d 506 (ED Va 2001), affirmed in part in *Cable News Network LP* v. *CNNews.com*, 56 Fed Appx 599 (4th Cir. 2003), where a website operated by a Chinese resident was subjected to the US Laham Act even though the site was in Chinese and accessed almost exclusively from China, no business was transacted in the US and there was no evidence that anyone in the US had actually accessed it. Discussed in Richard L. Garnett, 'Trademarks and the Internet: Resolution of International IP Disputes by Unilateral Application of US Law' (2005) 30 *Brooklyn Journal of International Law* 925, 934f.

[153] 714 NYS 2d 844 (1999). [154] *Ibid.*, 850.

foreseeability' is a legal decision – a legal decision as to what online providers ought to foresee, depending on the State's relative interest in the law's enforcement, balanced against its relative interests in protecting the online publishers from overregulation, and in protecting online activity generally.[155] In short, what is 'reasonably foreseeable' is the conclusion, not the starting point, of the inquiry. Consequently, it comes as no surprise that in respect of public law there is a marginally greater readiness to find that the law of a particular State was foreseeable. Courts in criminal matters make less of an attempt to soften the blow handed out by their rulings in favour of worldwide exposure. But ultimately the difference between the approaches taken to foreseeability in civil actions and criminal actions is one of degree.

Furthermore, considering the acceptability of the targeting approach in other private law contexts, as shown in Chapter 3, it is somewhat astonishing that it is generally rejected in private defamation actions.[156] But, given that defamation actions touch upon the fundamental value of freedom of expression and how that value should be balanced with competing rights, it is perhaps after all not surprising that States have been very concerned with protecting the particular way they have previously struck that balance. This by implication means that no foreign online inroads, however marginal, that would upset that traditional balance are acceptable.

The policy nature of 'foreseeability' also explains why the 'excuse' advanced by online publishers that they do not know the location of those who access their site has simply not been accepted by the courts. The legal insistence that the site was actually accessed in the forum in defamation actions has not gone hand in hand with a requirement that the publisher knew the location of the surfers. Thus it makes no difference in terms of the regulatory burden on online publishers if the whereabouts of the surfers are neither known nor can be controlled: worldwide legal compliance is still necessary. And for criminal purposes actual access is largely irrelevant for competence. There the accessibility of the site, the mere potential of an effect of the site on the State, is

[155] Larry Kramer, 'Rethinking Choice of Law' (1990) 90 *Columbia Law Review* 277, 336: 'the existence of "reasonable expectations" is not an objective question . . . [but] masks normative judgments reflecting what a court believes the parties ought to expect.'

[156] The more expansive approach is even more surprising given that these cases, as noted above, often concern not just jurisdiction but also applicable law, and thus one might legitimately have expected a more restrictive approach.

'harm' enough.[157] No actual effect, no hit on the site from the forum, is needed. This is in many ways not surprising, as the activity in question would have been criminalised precisely because it was considered so harmful as to require systematic regulation by the State rather than sporadic enforcement through private litigation. Mere accessibility as a connecting factor is also consistent with the general concern of criminal law to punish the defendant for his blameworthy behaviour,[158] as opposed to civil law which seeks to compensate the victim for actual harm suffered. Thus accessibility of a site is sufficient in criminal law and actual access tends to be necessary for civil law. Accessibility as a criterion for legal exposure makes foreseeability of foreign law extremely straightforward: every law is applicable (although it may lie dormant ready to strike should the need arise).

This goes to the heart of another pressing question: how can courts possibly pretend that actual compliance with the laws of all States is in fact feasible?[159] Is this a case of the emperor in his new clothes? The answer is that courts on the whole do not anticipate such compliance, but rather that online publishers should forego open access and territorially delimit their sites. Location-sensitive screening with the help of geo-location technology,[160] discussed in Chapter 7, is the only way to make the regulatory burden realistic. The French court very explicitly required Yahoo! Inc. to prevent access by users from French territory,

[157] This explains why manufactured contacts (i.e. contacts by the defendant with the forum State which were provoked by the plaintiff for the sole purpose of establishing a nexus with the State) are generally not sufficient in private cases but are sufficient in public cases.

[158] Consistent, for example, with *R* v. *Burdett* (1820) 4 B & Ald 115, which concerned a prosecution for seditious libel, which was held to be established without proof of 'publication' in the jurisdiction (here the County of Leicester). See also *R* v. *Treacy* [1971] AC 537, where a letter sent from England to blackmail a person in Germany was held to be within the criminal jurisdiction of England.

[159] Quite apart from the fact that compliance would also require compliance with the lowest common denominator, as argued e.g. in *R* v. *Perrin* [2002] EWCA 747, para. 35.

[160] Svantesson, above n. 68. See the discussion in Chapter 3 on how the zoning of online content allows for the operation of concurrent law and prevents conflicting regulatory claims. Already in 1996 *Playboy Enterprises Inc.* v. *Chuckleberry Publishing Inc.*, 939 F Supp 1032, para. III.B (SDNY 1996), put the onus on content providers to find the means to resurrect borders in cyberspace: 'While this Court has neither the jurisdiction nor the desire to prohibit the creation of Internet sites around the globe, it may prohibit access to those sites in this country. Therefore, while Tattilo may continue to operate its Internet site, it must refrain from accepting subscriptions from customers living in the United States.'

and investigated the feasibility of that order. The Australian policy statement on online offers of securities provides:

> In order not to target persons in Australia . . . the offeror must . . . take a variety of precautions designed to exclude subscriptions being accepted from persons in Australia and to check that the precautions are effective . . . Examples of precautions are not sending notices to, or not accepting applications from, persons whose telephone numbers, postal or electronic addresses or other particulars indicate that they are applying from Australia . . . It is not acceptable to only use precautions that place the responsibility on the applicant. For example, it is not enough to simply ask an applicant whether they are applying from Australia.[161]

Although the defendants in *People* v. *World Interactive Gaming Corp*. had implemented a screening mechanism, it was so easily circumvented that the court simply rejected the defendant's 'argument that it unknowingly accepted bets from New York residents. New York users can easily circumvent the casino software in order to play by the simple expedient of entering an out-of-state address.'[162] With these words, the court acknowledged both the importance of making the requisite connection knowingly and the need for reliable screening mechanisms, and this same approach with only the slightest variations applies also to civil cases.[163] Even if the courts do not specifically mention this as a solution, the implication of *Gutnick* or *Harrods* is simple: forego secondary targets of

[161] Australian Securities and Investments Commission, *Offers of Securities on the Internet*, Policy Statement 141 (10 February 1999, reissued 2 March 2000), PS 141.14. This statement also confirms that in the absence of location-sensitive mechanisms a site may be presumed to target Australia. Cf. ABA, above n. 57, 114: 'securities solicitation rules in the US, UK, and a number of other countries, attempt to distinguish between inadvertent contacts with a resident of the country from abroad (not regulated) and systematic efforts to target consumers in that country (which may be regulated).' But see also ABA, above n. 57, 113f, where it is noted that existing data-protection laws are triggered regardless of whether the collector of data-targeted the territory or not.

[162] NYS 2d 884, 851 (1999).

[163] Particularly in criminal law, legal responsibility for a site cannot be removed by the inclusion of a disclaimer or a request to the user to exit the site in certain circumstances. See e.g. Australian Securities and Investments Commission, *Offers of Securities on the Internet*, Policy Statement 141 (10 February 1999, reissued 2 March 2000), PS 141.14 and 141.15. Generally, see *Ticketmaster Corp*. v. *Tickets.com*, Lexis 4553 (CD Cal. 2000): 'It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site.' In the private context, the disclaimer may be relevant but must not be inconsistent with other evidence: *Tech Head Inc*. v. *Desktop Service Center Inc*., 105 F Supp 2d 1142 (D Or. 2000); *Euromarket Designs Inc*. v. *Crate & Barrel Ltd*, 96 F Supp 2d 824 (ND Ill. 2000); see also *Macquarie Bank* v. *Berg* [1999] NSWSC 526. Similarly, the screening of surfers

their sites such as Australia and the UK and simply not accept subscriptions from residents of 'marginally targeted' States. Implementing location-sensitive measures is vital both for the foreseeability of legal exposure as well as for making the regulatory burden manageable. The more reliable those measures, the greater the respect the law will accord to them.

Certainly, there is considerable pressure on freely accessible sites, especially those with 'legally significant' content, to drop the 'freely' and implement screening. But this simply begs the question: what is 'legally relevant' and how does one find out? This in turn brings us to the final part of this discussion: how do people normally foresee and know their legal obligations and how do these 'notice' mechanisms operate in the transnational world of the Internet?

4. Actually foreseeing and knowing foreign law

A. Actual notice and the effectiveness of law

While, as a matter of fairness, individuals should not be exposed to secret laws, that is, laws which are not foreseeable, the effectiveness of regulation demands more. It requires that the majority of those affected by it *actually* foresee and know the relevant rules. Although for a legal rule to be effective and to achieve its purpose,[164] there need not be 100 per cent compliance, still there is a need for it to be 'obeyed more often than not'.[165] On the other hand, large-scale non-compliance with any legal rule is problematic not just in terms of the failure of achieving the law's purpose, but also in terms of undermining the law's and regulator's credibility more generally. For laws to be obeyed, they certainly need to be known. The exception is indirect regulation: it needs to be neither foreseeable nor actually known to be effective.

must not merely be window-dressing: *Twentieth Century Fox Film Corp*. v. *iCraveTV*, US Dist. LEXIS 1013 (WD Pa, 28 January 2000), discussed in Svantesson, above n. 68, 129f; *Citron* v. *Zundel (No. 4)* (2002) 41 CHRR D/274, www.chrt-tcdp.gc.ca. See also ABA, above n. 138, 114f (in the data-protection context).

[164] Raz, above n. 17, 207.

[165] H. L. A. Hart, *The Concept of Law* (2nd edn, Oxford: Clarendon Press, 1994), 103. Hans Kelsen, *General Theory of Law and State* (Cambridge, MA: Harvard University Press, 1946), 39: 'Efficacy of law means that men actually behave as, according to the legal norms, they ought to behave, that the norms are actually applied and obeyed.' In this chapter, the terms 'conformity' and 'obedience' are used interchangeably denoting behaviour which is in accordance with the law, or, in psychological terms, with the 'abdication of initiative to an external source'. Stanley Milgram, *Obedience to Authority* (London: Tavistock, 1974), 114.

Indirect regulation has been described by Lessig, who argued that regulators are frequently more successful in achieving a desired outcome, not by having recourse exclusively to prohibitive rules backed by sanctions, but by using indirect laws which affect other possible constraints such as social norms, the market and the architecture.[166] An advantage of such indirect regulation is that the prohibitive rules are either unnecessary or merely supplementary, facing an environment within which conformity is already largely established. If the government wants people to wear seatbelts, it can make it an offence not to wear one (direct regulation) or – more indirectly – it can educate the public on its benefits (i.e. influence social norms), oblige insurance companies to give better rates to seatbelt wearers (i.e. influence the market) or mandate cars with automatic seatbelts (i.e. influence architecture).[167] One problem or advantage, as the case may be, of any indirect regulation is transparency, or rather the lack of it.[168] The effectiveness of indirect regulation of relevant market, social norms and architecture does not depend at all on the visibility of the law and at times even positively benefits from its invisibility, however controversial.[169] The object may be achieved without individuals having actual notice of the content, or even the existence, of those indirect laws, with their choices between possible alternative courses of action being directed one way or another by market forces, social norms and architecture.

As much as the visibility of the law is not a prerequisite for the effectiveness of indirect regulation (which provides another reason why governments may find it attractive), it is essential for direct regulation. Here the law is not channelled through an external order such as the market or social norms, but seeks to impact on conduct directly. For those norms it is indispensable that they are at least actually known; even more so if the legal subject is not subject to other influences or constraints on his behaviour such as the market or moral norms – as is frequently the case in the transnational online context. And depending on what theory one adopts on why people obey laws, such visibility of, and familiarity with, the law may go quite a way towards obedience.

[166] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Book, 1999), 90ff.

[167] *Ibid.*, 93f. [168] *Ibid.*, 98. See also Chapter 1.

[169] *Ibid.*, 96, citing as an example the Reagan administration's indirect strategies to reduce the number of abortions.

Very briefly, the traditional and still commonly held Austinian school of thought is that the fear of sanctions provides the necessary inducement for obedience: it is not the actual sanction being applied, but the threat of it.[170] Clearly, this can only work if individuals have notice of the nature of the sanction and in what circumstances it may arise: 'This punishment then . . . in order to produce its effect must in some manner or other be announced: Notice of it must in some way or other be given, in order to produce an expectation of it, on the part of the people whose conduct it is meant to influence.'[171] The effectiveness of the law in question depends on publicising the content of the rule in question, as well as the sanctions for its breach, so that individuals are not only conscious of the legal consequences that may attach to certain conduct, but also know how they can avoid being subjected to it. If this theory holds true, an immediately obvious problem in the online context is the territorially limited reach of the State's enforcement power, which would mean that foreign online actors have often no motive to comply with laws that cannot be enforced against them. But is obedience indeed based on the fear of a likely sanction being imposed in the case of non-compliance?

Many eminent legal philosophers and legal sociologists[172] have disputed that people obey law out of a fear of sanctions. Hart argues that sanctions are 'required not as the normal motive for obedience, but as a *guarantee* that those who would voluntarily obey shall not be sacrificed to those who would not. To obey, without this, would be to risk going to the wall.'[173] He asserts that obedience to the law is generally voluntary, based upon, for example, a cost–benefit analysis, a disinterest in the welfare of others or a respect for the rules themselves.[174] This last motive, namely, the idea of law itself furnishing the motive for lawful

[170] In Bentham's language, the fear of pain; and, for that fear to be induced, the punishment must be announced to those expected to comply with the relevant law. H. L. A. Hart, *Essays on Bentham* (Oxford: Clarendon Press, 1982), 109, 127ff, where he also refers to the prospect of a reward for compliance as a possible motive for obedience. Johnson and Post, above n. 23, 1369: 'Law-making requires some mechanism for law-enforcement, which in turn depends on the ability to exercise physical control over, and impose coercive sanctions on, law-violators.' In the context of businesses, the widely held law-as-price theory suggests that businesses obey the law only if conformity would be more profitable than violation. For a criticism of this view, see Cynthia A. Williams, 'Corporate Compliance with the Law in the Era of Efficiency' (1998) 76 *North Carolina Law Review* 1265.

[171] J. Bentham, *Of Laws in General* (ed. by H. L. A. Hart, London: Athlone Press, 1970), 134.

[172] For example, Eugen Ehrlich in Kelsen, above n. 165, 24ff.

[173] Hart, above n. 20, 198 (emphasis in the original).

[174] *Ibid.*, 197.

conduct,[175] seems to be captured by what Austin calls habitual obedience.[176] Kelsen seems to agree, although doubting that it provides the only motive for obedience:[177] '[i]n all probability ... the motives of lawful behavior are by no means only the fear of legal sanctions or even the belief in the binding force of the legal rules.'[178]

What does belief in the binding force of legal rules actually entail? Milgram showed with experiments that individuals may voluntarily obey a command in the absence of sanctions or concurrent moral beliefs when the command comes from what they perceive to be a legitimate authority.[179] And such perception triggers voluntary obedience which, unlike coerced obedience, does not require constant direct surveillance: 'When the gunman leaves, or when his capacity for sanction is eliminated, obedience stops. In the case of voluntary obedience to a legitimate authority, the principal sanction for disobedience comes from within the person. They are not dependent upon coercion, but stem from the individual's sense of commitment to his role.'[180] He shows that '[i]t is the appearance of authority and not actual authority to which subjects respond'.[181] In the transnational Internet context, this appearance of authority may be absent: individuals may often not accept that a foreign State has or should have any legitimate authority over them, quite

[175] Kelsen, above n 165, 40, notes, however, at 15: 'There are hardly any norms whose purport appeals directly to the individual whose conduct they regulate so that the mere idea of them suffices for motivation.'

[176] J. Austin, *The Province of Jurisprudence Determined* (ed. by H. L. A. Hart, London: Weidenfeld & Nicolson, 1954), 198: 'The *bulk* of the given society are in a *habit* of obedience or submission to a *determinate* and *common* superior' (emphasis in the original). But note D. A. Freeman 'Milgram's Obedience to Authority – Some Lessons for Legal Theory' (1979) 1 *Liverpool Law Review* 45, 54: 'Austin does not deny this essential element of legitimacy: his habit of obedience is recognition that coercive commands will fail if the commander does not also command broad social acceptance. Yet few would deny that the concept of authority is insufficiently delineated in Austin's theory.'

[177] Kelsen, above n. 165, 24. He also averts to what Lessig would call market forces, saying that a person may pay his or her debts based on the fear of a commercial sanction in the form of a loss of credit rather than because of a fear of legal sanction for non-payment; or what Lessig would call social norms, saying that lawful behaviour might be induced by moral or religious beliefs which may require the same conduct as that required by the legal rule.

[178] *Ibid.*

[179] Milgram, above n. 165, 138f, also at 8: 'it is a fundamental mode of thinking for a great many people [that] once they are locked into a subordinate position in a structure of authority that they comply with the demands made by that authority.'

[180] *Ibid.*, 140f. [181] *Ibid.*, 140.

regardless of the actual legal position. The frequent lack of an effective sanction against the foreign violator may consolidate that mistaken belief,[182] which again suggests that sanctions play a role, albeit more indirectly, even in respect of voluntary obedience.

So, at the risk of stating the obvious: actual notice of legal rules is absolutely critical for the effectiveness of direct regulation. It is a minimum prerequisite for achieving obedience, and is possibly even sufficient. Certainly, discussions about the enforceability of foreign laws or the lack of enforcement mechanisms should start from the premise that most legal subjects want to obey the law and then ask the question if such obedience is realistically facilitated in the transnational online context. This is the final issue in this chapter: how accessible are foreign legal norms in fact? Can online actors actually foresee and know them?

B. Traditional methods of publication of law

States expect that foreigners who target or 'enter' territory with a website must comply with local norms – just like traditional transnational entrepreneurs. If that is the case, the State must also make these norms accessible to them. And here it is important to repeat that many of the online actors are not like all their traditional giant counterparts, but are small-to-medium actors for whom one set of local rules often proves burdensome and requires significant efforts by the State to ensure compliance.[183] Even the online giants like Amazon, eBay or Google are heavily burdened by that insistence[184] – yet at least they tend to have the

[182] This concern is implicit in Raz' critique of Austin's definition of law in Joseph Raz, *The Concept of a Legal System* (Oxford: Clarendon Press, 1970), 14f: 'Of course Austin knows that "in many cases the positive law of a given independent community imposes a duty on a stranger". He explains the difficulty by introducing the concept of partial or limited membership in a society. A stranger is a partial member in so far as he is susceptible to the sovereign's power. Instead of saying that only commands addressed to subjects are law, it would be more precise to say that *a command is law only if it is addressed to people who are likely to suffer the prescribed sanction, in case this should become necessary*' (emphasis added, footnotes omitted).

[183] For example, a survey by the Australian Competition and Consumer Commission found that more than 50 per cent of the Australian sites surveyed which sold goods or services illegitimately attempted to disclaim consumers' warranty rights or limit liability. See ACCC, 'ACCC Issues Warning to On-line Traders: "Shape-up" Sites' (25 June 2004), www.accc.gov.au/content/index.phtml/itemId/519730/fromItemId/2332/.

[184] This is reflected, for example, in the number of high-profile publishers who intervened in *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56.

local legal machinery to ensure compliance. In any event, the fact that more actors have to comply with more sets of rules creates the imperative to make these rules more easily accessible.

How do legal subjects normally find out about their legal obligations? In the local context much of the law will not require active publicity after perhaps an initial period following its introduction, but is known simply through common knowledge:

> The law must be made available for anyone, at least anyone with a good lawyer, to peruse and discover. But passive publicity of this sort seems an inadequate substitute for active publicity unless something alerts us that we ought to look at the law. In the case of many laws, this is no problem, either because their existence is common knowledge – we all know that there are laws against smuggling ... or because the law codifies a universally recognised moral obligation.[185]

Generally, notice of legal rules occurs in more subtle ways than through people reading about them through official sources. Even when common knowledge of rules does not provide individuals with knowledge of the intricacies of those rules, it nevertheless serves as an alerting device. It alerts us to the possibility of regulation in respect of certain activities, things and matters. For example, in Britain there would not be an expectation of regulation in respect of meetings in a public place or political commentary; but in respect of owning or selling firearms there clearly is, so much so that anyone wanting to acquire one could reasonably be expected to inform himself of his legal duties.[186] But would they indeed need to go to that effort?

In respect of much regulation, there are hotspots of knowledge that effectively absolve others from the burden of having to know. Often these intermediaries also ensure legal compliance by others through legal restrictions on their own activities.[187] For example, a shop-owner selling firearms will inform prospective buyers of their rights and duties

[185] David Luban, 'The Publicity of Law and the Regulatory State' (2002) 10 *Journal of Political Philosophy* 296, 297.

[186] Note *Staples* v. *US*, 511 US 600 (1994), discussed below.

[187] 'It is rather easy to observe that the largest part of behaviour regulation is not generated in today's capitalist societies by the relational networks of sociality but as a result of operating within institutional frames of activity.' Michalis Lianos, 'Social Control after Foucault' (2003) 1(3) *Surveillance and Society* 412, 414, www.surveillance-and-society.org. See also L. Hancher and M. Moran, 'Organizing Regulatory Space', in Robert Baldwin, Colin Scott and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: Oxford University Press, 1998), 148.

in relation to firearms, and not sell them a firearm (being prohibited from doing so) unless they meet the legal prerequisites. A chemist knows what drugs can be sold to whom, when and in what quantities. A news agency, bookshop or TV company knows which publications or programmes are legal or restricted, and a publican knows to whom alcohol may or may not be served or what games may or may not be played on the premises.[188] And often these hotspots are mere links in a much longer chain along which regulation occurs and notice expectations are spread. So the chemist can rely on the licensed drug manufacturer or distributor to offer and sell only approved drugs and the news agency can rely on newspaper publishers to know the rules on defamation or obscenity. In short, law-makers often rely on structure and hierarchies along which the need-to-know is spread and often shifted away from the ultimate end-user.

Common knowledge either provides subjects with the content of legal norms (e.g. the rule against stealing or selling heroin) or alerts them to the possibility of regulation (e.g. possession of firearms). Also the onus to find out about the legal norms is often shifted away from the individual to higher links in the transactional chain. The question is how these notice devices function in the global online village.

C. The failure of traditional methods in the online world

The answer is: not very well. Beyond a core of universally accepted norms, for example those against theft, murder or breaching contractual promises,[189] there is very little in the way of a global common knowledge serving as an alert system; and this also applies to commercial activity where, in particular, consumer protection regulation varies significantly from State to State. So, in respect of those very areas where States do not share harmonised rules and where online actors would need to know about the divergent standards, there is no global common knowledge to alert a person to the legal requirements alertness. This is particularly troublesome for smaller online actors who do not have the benefit of in-house legal advice.

[188] At times this may also involve public agency, e.g. a social security agency, which means that the law does not require self-application by citizens.

[189] For an excellent evaluation of the extent of harmonised legal standards, see Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cybercrime?' (2002) 10 *International Journal of Law and Information Technology* 139.

It may be argued that there is certainly a global consciousness that rules vary from place to place and that this should be enough to put individuals and businesses on enquiry as to the foreign legal norms when going online. There are two problems with that argument. First, although online actors may know in principle that rules are different elsewhere, in the particular circumstances our legal imagination is often too tied up with our local common knowledge even to predict the possibility of a divergent foreign legal standard. As argued above, it is unlikely to occur to publishers in the UK to check Chinese defamation standards when writing about a dead Chinese person simply because under the common law you cannot defame the dead.[190] In the US, where public figures are subjected to very robust free speech, smaller publishers might never stop to think that other States might not recognise the 'obvious' distinction between private and public figures. In a State where the laws do not distinguish between consumers and businesses in commercial transactions, it is unlikely that locals would foresee that other States might make that distinction. Secondly, and more worryingly, it is doubtful whether many of the smaller online businesses and publishers even realise that foreign law may apply to their online activities, which makes the substantive foreign law even less accessible.[191]

Perhaps the main purpose underlying cases like *Yahoo* and *Töben*, which stood next to no chance of being enforced, was nothing other than to put online publishers around the world on notice about French or German law on extremist right-wing speech as well as potential legal exposure by virtue simply of web presence. Interestingly, the French court in May 2000 ordered the publication of an abstract of the order to be pronounced in five daily or weekly newspapers chosen by the plaintiff.[192] Similarly, the civil plaintiffs asked the French court in the Timothy Koogle prosecution to publish any future judgments in four

[190] See above nn. 95–6 and the accompanying text. Sallie Spilsbury, *Media Law* (London: Cavendish, 2000), 77: the 'reputation of a dead person is deemed to die with him'. For the very different interpretations of obscenity, see e.g. Karsten Bremer, *Strafbare Internet-Inhalte in International Hinsicht – Ist der Nationalstaat wirklich überholt?* (Frankfurt a. M.: Peter Lang Verlag, 2001), 138ff, http://ub-dok.uni-trier.de/diss/diss60/20000927/20000927.pdf.

[191] To make foreign substantive law accessible, it is necessary that online publishers realise that foreign substantive law may be applicable to them.

[192] *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000).

French newspapers, one newspaper of a Member State of the European Union, in the European and American editions of the *New York Times* and *Wall Street Journal*, as well as on the yahoo.com and yahoo.fr websites.[193]

The absence of a global common knowledge is not the only problem creating new 'notice' imperatives for the online world. Traditional legal hierarchies, where intermediaries carry the 'notice' burden on behalf of other businesses or end-users, have also broken down in the online global village. This is illustrated, for example, by the fairly common clause in Marks & Spencer's Terms and Conditions:

> Marks & Spencer make no representation that any products or services referred to in the materials on this website are appropriate for use, or available, in other locations. *Those who choose to access this site from other locations are responsible for compliance with local laws if and to the extent local laws are applicable.*[194]

Similarly, Amazon.co.uk's Conditions of Use and Sale include the following:

> Additionally, please note that when ordering from Amazon.co.uk, you are considered the importer of record and must comply with all laws and regulations of the country in which you are receiving the goods.[195]

These clauses show that even substantial businesses are overwhelmed by the global regulatory requirements and that they attempt to handle it by shifting the notice and compliance burden to the foreign end-user. Whether these clauses are in fact effective in absolving them from possible breaches of 'excluded' foreign law is questionable[196] as generally it is not possible to contract out of public law or some private law, such as defamation law. In particular, though, for small online businesses and publishers, such clauses might be the only realistic answer to the legal 'expectation' overload. In any event, their use may indeed be legally defensible in so far as

[193] *R* v. *Timothy K and Yahoo Inc.* (Tribunal de Grande Instance de Paris, 26 February 2002, No. 0104305259), www.foruminternet.org/actualites/lire.phtml?id=273/.

[194] Marks and Spencer, Terms and Conditions, www.marksandspencer.com (emphasis added).

[195] Amazon, Conditions of Sale and Use, www.amazon.co.uk, clause 16.

[196] It made no difference in the case of *State of Minnesota* v. *Granite Gate Resorts Inc.*, 568 NW 2d 715, 717 (1997), where a note on the offending website 'advised users to consult with local authorities regarding restrictions on offshore sports betting by telephone before registering with WagnerNet'.

it applies to foreign laws that are insufficiently accessible to the online business. For States, this abdication of responsibility (whether legally valid or not) by the traditional intermediaries, particularly to the rather unreliable end-users, is worrying as the latter may be neither able nor willing to inform themselves and comply. It is like letting the owner of the firearms shop sell firearms to everyone with the proviso that it is up to them to comply with the law – no doubt the number of illicit firearms would drastically increase. But equally, from the perspective of the law-abiding citizen, these clauses expect rather too much and frequent accidental non-compliance is also likely to ensue.

The reality is that the global village lacks key 'notice' mechanisms – such as common knowledge and knowledge hotspots – which in the domestic context play a critical role either in bringing rules to the attention of their subjects or in relieving them of knowing them. States have a responsibility and a self-interest in bringing their rules home to online actors if they expect compliance with them. Any realistic debate on Internet governance, and in particular on the legal obligations of online actors under foreign law, must be sensitive to these more subtle concerns. It is simply wrong to assert that there are no 'decisive factors as to why e-commerce should be treated any differently from transactions that are not carried out by electronic means'.[197] There are.

Perhaps a final illustrative case speaks louder than any theoretical argument. In *Staples* v. *US*,[198] the US Supreme Court had to deliberate on the issue of whether owning an assault rifle is conduct that should have put the accused on notice about the possibility of State regulation. It concluded that 'buying a shotgun or rifle is a simple transaction that would not alert a person to requirements any more than would buying a car'.[199] Interestingly, the common knowledge, or the lack thereof, provided, in the eyes of the judges, an excuse for non-compliance. But, even more astonishingly, at least from a European perspective, is that US common knowledge would not have rung alert bells as to the possibility of regulation in respect of guns. In Europe, alert sirens would have been howling. It is not difficult to see how in the transnational online context online publishers tied up in their local mindset frequently fail to predict that their online conduct is 'legally relevant' elsewhere.

[197] Oren, above n. 10, 670.
[198] *Staples* v. *US*, 511 US 600 (1994), discussed in Luban, above n. 185, 303ff.
[199] *Staples* v. *US*, 511 US 600, 614 (1994).

5. An afterthought

Do all these arguments about principle really matter? Is the vast majority of websites – personal, educative, commercial or local community websites – not rather 'harmless' from any State's perspective? Most States not only would lack the actual power (i.e. enforcement jurisdiction) to regulate them in fact but also would have no interest at all in doing so. So does it really matter that, in those relatively few instances when a website is 'harmful' and when there is some possibility of enforcing regulatory claims against the foreign controller (or when that enforcement is of secondary importance as is often so in defamation disputes), States make these sweeping regulatory assertions?

The answer is yes, it does matter. First of all, there is a legitimate expectation that law is on the whole rationally defensible, that it has integrity. You cannot reasonably defend an irrational legal position on the basis that on the whole it is ineffectual, that most activity is not affected by it. Secondly, the legal position that every website is subject to the laws of every State is irrational because theoretically it is inconsistent with the system of sharing regulatory competence between States depending on the relative strengths of their connections with the controversial facts. It is also irrational because for the vast majority of online publishers compliance is simply a practical impossibility. Thirdly, one could reverse the argument: if States have in reality no real interest and no real power to regulate the vast majority of foreign sites, would it not be more appropriate to frame assertions of regulatory competence in those relatively isolated instances in such a way as to reflect that general reality? Should the law not simply acknowledge that a French village website for local mushroom enthusiasts is only subject to French law, quite irrespective of the fact that in principle in may be accessed by someone in Brazil, Vietnam or Finland. Currently, that obvious legal conclusion is not supported by case law or legislative practices and that is unfortunate.

5

The solution: only the country of origin?

1. The *exclusive* country-of-origin approach

Online publishers have argued that – instead of looking to the destinations of their online activities to determine their legal exposure (i.e. adjudicative and/or legislative jurisdiction[1]) – regulatory competence should only lie with the State where their activities originate.[2] They argue that it should only be their home State where *for legal purposes* a website is 'published', a trademark is 'used', an advertisement or offer for sale is 'displayed', an online contract is 'concluded' and so on. The distinct advantages would be that online publishers could easily foresee their legal exposure and the regulatory burden would be realistic. It is a simple principle which creates predictability and certainty for all concerned, and the 'origin' State is able to enforce its laws against the local publisher and would not be plagued by the enforcement problems faced by 'destination' States. These are persuasive arguments and, yet, as the discussion in previous chapters and below shows, the times when they have found fertile ground are few and far between. States have on the

[1] See Chapter 1, section 2.A, above.

[2] In both civil and criminal cases, such as Dow Jones in *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56 or Perrin in *R* v. *Perrin* [2002] EWCA 747. The relative merits of the country-of-origin approach have been subject to much academic debate in various online contexts: Graham J. H. Smith (ed.), *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002), 532f; Michael S. Greve, 'If It Ain't Broke, Why Is Everyone Trying to Fix It? Taxing E-Commerce in a Destination-Based World', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: Cato Institute, 2003), 269; Julia Hörnle, 'Country of Origin Regulation in Cross-Border Media: One Step Beyond the Freedom to Provide Services?' (2005) 54 *International and Comparative Law Quarterly* 89; Lokke Moerel, 'The Country-of-Origin Principle in the E-Commerce Directive: The Expected One Stop Shop' (2001) 7 *Computer and Telecommunication Law Review* 184; Karsten Bremer, *Strafbare Internet-Inhalte in Internationaler Hinsicht – Ist der Nationalstaat wirklich überholt?* (Frankfurt a. M.: Peter Lang Verlag, 2001), 173ff, http://ub-dok.uni-trier.de/diss/diss60/20000927/20000927.pdf.

whole not been prepared to forego regulatory competence in favour *solely* of the State of origin.

This is not to say that the States of origin have not asserted regulatory control over local online publishers. They have, but they have not done so exclusively. Online publishers are generally subjected to the laws of both where their activities originate *and* where their activities have an effect (the latter at least in principle).[3] This position is entirely consistent with the fundamental notion that the territorially defined State has, at least theoretically, control over whoever is, and whatever occurs, on its territory. Traditionally, the places where an actor acted and where his acts took effect were almost always one and the same, leaving little room for the origin-versus-destination dichotomy. This dichotomy developed with advances in communication technology and greater movement of persons, property and goods across borders. As shown in Chapter 3, the expansion of traditional territorial tests has focused on the 'destination' side of the coin – by seeking to catch activities of foreign origin which had an effect on local territory. On the other hand, the 'origin' side of the dichotomy has remained virtually unaffected by those technological, economic and social changes. This is not surprising given that the State asserting competence over a local actor would not be too concerned whether or not his activities also had an extraterritorial effect.[4] However, the discussion below shows that, within a more cooperative framework, increasing transnationality could, and perhaps should, change how States interpret their regulatory power and arguably concomitant responsibility in respect of activities originating in their territory.[5]

For the moment, what is significant is that regulatory assertions by the State of origin and by the States of destination have generally, in the offline and online context, run concurrently across the regulatory board. But, there are a few exceptions – exceptions in which competence has been reserved exclusively to the State of origin. Despite the strong

[3] For more examples supporting the latter proposition, see Bremer, above n. 2, 117ff.

[4] Particularly as criminal law often focuses on the blameworthy act rather than its consequences. In *R* v. *Treacy* [1971] AC 537, the offence of blackmail was committed where the last irrevocable step was taken in the making of the demand. The fact that the demand was received in Germany was irrelevant.

[5] This aspect is rarely mentioned, let alone explored. Exceptionally, in the context of transnational environmental harm, see International Law Association, *First Report by the Committee on Transnational Enforcement of Environmental Law* (2002), www.ila-hq.org/html/layout_committee.htm.

pressure on destination-focused tests, these instances are so rare that one has to ask why in those few instances the exclusive country-of-origin approach is in fact acceptable. When does it provide an acceptable response to the shortcomings of the destination approach? Why has it not, and will it not, take a front seat in online governance?

This chapter explores the exclusive country-of-origin approach (hereinafter, origin rule or principle) in the particular context of online gambling regulation,[6] although, as in previous chapters, the arguments are on the whole not peculiar to gambling. Online gambling provides an appropriate context, first, because it has triggered a flurry of legislative activity in many States in addition to numerous and some high-profile cases. Gambling generates significant economic activity, employment and revenue, and thus it illustrates perfectly the financial factors impacting on competence decisions.[7] Equally, gambling produces significant harm flowing from gambling addictions. There are no simple regulatory answers, and in fact there has been very little consensus among States as to the right kind of regulation. These are matters of substantive law that are not reviewed here. The focus, in accordance with the subject of this book, is entirely on competence. However, the regulatory diversity amongst States highlights the difficulties they face in upholding and enforcing their peculiar national law in spite of the global Internet. Particularly in the context of public or criminal law, which moves centre-stage in this chapter, the reality is that States face even greater problems than they do in civil law, in trying to enforce their local laws and policies when the offending actors are not present and have no assets within their territory.

Secondly, online gambling regulation supplies one of the rare instances of the exclusive country-of-origin approach: the UK Gambling Act 2005 (hereinafter, the Act).[8] The UK approach – unusual

[6] For a recent discussion, see Christine Hurt, 'Regulating Public Morals and Private Markets: Online Securities Trading, Internet Gambling and the Speculation Paradox' (2005) 86 *Boston University Law Review* 371. For an early paper, see Jack Goldsmith, 'What Internet Gambling Legislation Teaches About Internet Regulation' (1998) 32 *The International Lawyer* 1115.

[7] Another highly profitable online activity is the sale of pharmaceuticals: see e.g. Phil Ayres, 'Prescribing a Cure for Online Pharmacies' (2005) 72 *Tennessee Law Review* 949. Recent competence cases concerning cross-border drug sales include: *Deutscher Apothekerverband eV* v. *0800 Doc Morris NV*, Case C-322/01 [2003] ECR I-14887; *Arzneimittelwerbung im Internet* (BGH, 30 March 2006, I ZR 24/03), below n. 87.

[8] The Act applies in England, Scotland and Wales; thus it would be more accurate to talk about the British legislation, but for convenience the discussion refers to the UK.

not just for adopting the exclusive country-of-origin approach but also for its cooperative stance – forms the cornerstone of this chapter, and is compared and evaluated against conventional approaches. The discussion below is divided into what are effectively two sides of the same coin: first, how do States deal with foreign online gambling providers who carry on their activities within the State, and secondly and rarely noted, how do they deal with local online gambling providers who offer their services elsewhere? This second aspect foreshadows what is more fully explored in Chapter 6, namely, enforcement jurisdiction.

2. Online gambling: foreign providers' local activities

A. *The general rejection of the exclusive country-of-origin approach*

In the gambling context, as in respect of most other laws, States have almost invariably rejected the exclusive country-of-origin approach, and sought to impose their domestic policies on foreign operators on the basis that their activities have an effect within the State's territory. Any operator – regardless of its location within or outside the jurisdiction – must comply with the law of the State within which it offers gambling services.

Netherlands and Germany

A typical example is the Dutch case of *National Sporttotaliser Foundation* v. *Ladbrokes Ltd*,[9] where the defendant, Ladbrokes, based in England and Gibraltar, was ordered by a Dutch District Court to make its gambling site inaccessible to Dutch residents, on the basis that it did not comply with Dutch licensing requirements and with norms of good conduct in dealing with competitors. Along the same lines, a court in Hamburg held in 2004 that an Austrian company breached German penal law by

Explanatory Notes to Gambling Act 2005, www.opsi.gov.uk/ACTS/en2005/2005en19.htm. For useful background documentation, see Department for Culture, Media and Sport, *Gambling Review Report* (July 2001); *A Safe Bet for Success – Modernising Britain's Gambling Laws* (March 2002); *The Future Regulation of Remote Gambling: A DCMS Position Paper* (April 2003); *Modernising Britain's Gambling Laws – Draft Gambling* Bill (July 2003); *Draft Gambling Bill – Regulatory Impact Assessment* (November 2003); *Draft Gambling Bill – Explanatory Notes* (November 2003), all available at www.culture.gov.uk/gambling_and_racing/gambling_bill.htm; Joint Committee on the Draft Gambling Bill, *First Report* (25 March 2004), www.parliament.the-stationery-office.co.uk/pa/jt/jtgamb.htm.

[9] District Court, The Hague, 27 January 2003, www.rechspraak.nl; see also *Holland Casino* v. *Paramount Holdings* (District Court, Utrecht, 27 February 2003).

offering online sports-betting services in Germany without the requisite local licence, despite it holding a bookmaker licence under Austrian law.[10] In both cases, the fact that the foreign providers were licensed under the laws of another EU member made little difference. These are classic instances of the concurrent application of the laws of the origin State and the destination State.

European Union

Even in the EU, the destination principle is still, at least in the gambling context, perceived as vital to protect national moral and economic interests. Thus gambling was excluded from the scope of the Electronic Commerce Directive,[11] which provides another instance of the origin approach to online regulation, further discussed below. Although the Directive does not apply to gambling, in 2003 in *Gambelli*[12] the European Court of Justice was presented with an attempt to introduce the exclusive country-of-origin approach to gambling via the back door. The defendants in the Italian criminal proceedings were Italian agencies which acted as intermediaries for the UK-licensed bookmaker, Stanley International Betting Ltd; they channelled bets via the Internet from Italy to Stanley contrary to local licensing requirements. It was argued that Italy – by maintaining a national monopoly in the betting and gaming sector in respect of sporting events, enforced through criminal sanctions against unlicensed providers as well as punters[13] – imposed on foreign providers an unjustified restriction on their freedom of establishment and freedom to provide services, contrary to Articles 43 and 49 of the EC Treaty. Those freedoms, it was asserted, demanded that Member States take a regulatory hands-off approach in relation to gambling services originating from, and properly regulated by, another Member State: 'Stanley, which operates entirely legally and is duly regulated in the United Kingdom, should [not] be treated by the Italian legislation in the same way as an operator who organises clandestine gaming,

[10] *Unzulässiges Online-Glücksspielangebot* (OLG Hamburg, 19 August 2004, 5 U 32/04) (2004) 12 *Computer und Recht* 925; following *Schöner Wetten* (BGH, 1 April 2004, I ZR 317/01).

[11] Recital 16 and Art. 1(5)(d) of the Electronic Commerce Directive, 2000/31/EC. implemented in the UK by the electronic Commerce (EC Directive) Regulations 2002, SI 2002/2013, see reg. 3(1). *The Future Regulation of Remote Gambling*, above n. 8, paras. 115, 116, noting that the exclusion of gambling from the Directive was based on the lack of harmonisation.

[12] *Criminal Proceedings against Piergiorgio Gambelli*, Case C-243/01 [2003] ECR I-13031.

[13] Art. 4 of Law No. 401/89.

when all the public-interest concerns are protected by the United Kingdom legislation'.[14]

In economic terms, the case concerned the legitimacy of a State monopoly on betting *vis-à-vis* competitors from other EU States. The court held that the State monopoly backed by criminal sanctions imposed a restriction on both the freedom of establishment and the freedom to provide services, but those restrictions may be justified 'as exceptional measures expressly provided for in Articles 45 and 46 . . . or justified . . . for reasons of overriding general interest'.[15] Restrictions on foreign gaming providers would be justified if they 'reflect a concern to bring about a genuine diminution of gambling opportunities',[16] but would not be justified if they were motivated simply by a fear of reduced revenues.[17] So the freedoms under the EC Treaty do not prevent Member States from seeking to regulate foreign gambling providers, provided the main objective is not economic. In the end, '[i]t is for the national court to determine whether such legislation . . . actually serves the aims which might justify it, and whether the restrictions it imposes are disproportionate in the light of those aims'.[18] The court in the above-mentioned German judgment determined that the German licensing requirements imposed on gambling providers from other Member States were not inconsistent with *Gambelli*.[19] Of course, *Gambelli* does not at all restrict Member States as far as providers from outside the EU are concerned, even if motivated purely by a desire to protect internal revenues.

United States

Across the Atlantic in the US, which has also sought to restrict online gambling, there are quite a number of cases where foreign providers have been held subject to US domestic gambling restrictions. In *US* v. *Ross*,[20] Ross, the manager of Island Casino, was charged with the offence of using wire communication facilities for the transmission of bets or wagers. Island Casino, an entity operating from Curacao in the Netherland Antilles, had set up a site promoting gambling and inviting punters to place bets via a toll-free number. Some of those punters were undercover agents in New York who were able to place bets with it. Ross

[14] *Criminal Proceedings against Piergiorgio Gambelli*, Case C-243/01 [2003] ECR I-13031, para. 28.
[15] *Ibid*., para. 60. [16] *Ibid*., para. 61. [17] *Ibid*., paras. 61f. [18] *Ibid*., para. 76.
[19] *Unzulässiges Online-Glücksspielangebot* (OLG Hamburg, 19 August 2004, 5 U 32/04) (2004) 12 *Computer und Recht* 925, para. II.2.g (bb) and (cc).
[20] WL 782749 (SDNY 1999).

tried to argue that the court lacked subject-matter jurisdiction because '[his] activities occurred in Curacao ... [and] it is not clear whether Congress would have wished the precious resources of United States courts and law enforcement agencies to be devoted to them'.[21] While it was very noble of Ross to think of the court's resources, not surprisingly the court found that the language of the statute clearly suggested the contrary and thus that it had subject-matter jurisdiction. In *People* v. *World Interactive Gaming Corporation*,[22] an Antiguan company was enjoined from offering its online gambling services to residents of New York state.[23] The fact that the activities originated offshore and were legal there, was held to be irrelevant. The court endorsed a clear-cut country-of-destination approach when it noted that 'under New York Penal Law, if the person engaged in gambling is located in New York then New York is the location where the gambling occurred'.[24] Similar actions have been successfully brought in Missouri and Minnesota.[25]

More recently, in *US* v. *American Sports Ltd*,[26] the US Court of Appeals upheld the right of the government to seize funds in a US bank account which was established in relation to illegal gambling activities in New Jersey via a New Jersey company acting on behalf of an English enterprise. The gambling was promoted through the Internet and carried out via the telephone. The court rejected the argument that, as the gambling transaction is concluded where the bet or wager is accepted, in this case England, 'no illegal gambling activity had occurred at all ... because gambling is legal in England, and all of the actors there were legally licensed to conduct a gambling business'.[27] To support that argument, the appellants *inter alia* claimed that 'one sovereign cannot

[21] *Ibid*., 8. [22] 714 NYS 2d 844 (1999).

[23] But note the Antiguan corporation was the wholly owned subsidiary of a Delaware corporation that maintained its corporate offices in New York.

[24] *People* v. *World Interactive Gaming Corp*., 714 NYS 2d 844, 850 (1999). In a civil action, the court may have come to a different conclusion and followed the parties' choice of forum and law, often that of the origin State.

[25] *US* v. *Cohen*, 260 F 3d 68 (2d Cir. 2001); *State of Missouri* v. *Coeur d'Alene Tribe*, 164 F 3d 1102 (1999); *State of Missouri* v. *Interactive Gaming & Communications Corp*., WL, 33545763 (Mo Cir. 1997); *State of Minnesota* v. *Granite Gate Resorts Inc*., 568 NW 2d 715 (1997). See also American Bar Association, 'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf, 144ff.

[26] 286 F 3d 641 (2002).

[27] *US* v. *American Sports Ltd*, 286 F 3d 641, 650 (2002). Cf. *State* v. *Truesdale*, 152 F 3d 443 (5th Cir. 1988), where the court had held, in the case of bets being placed through phone calls from Texas to the Dominican Republic and Jamaica, that the actual

criminalize gambling activity that is legal under the law of another sovereign'.[28] Clearly, they had not done their homework. Interestingly, the appellants also argued that, as gambling was to some extent permitted in New Jersey, the court – in the name of comity or good neighbourliness – should defer to the appellants' British licences to conduct a gambling enterprise. Yet again, the argument was rejected: 'These legislative enactments reflect the "strong public policies" of the United States government, and the government is not required to tolerate activity that it defines as illegal merely because it affects some who may live in a country where the activity is legal.'[29]

Given that there is no general ban on traditional gambling in the US, one cannot but wonder what 'strong public policies' make online gambling facilitated by offshore providers so abhorrent. The answer is: national economic interest. In respect of the US attitude it was suggested:

> The fairly harsh approach to online gambling is a reversal of both the federal government's . . . receptivity to tribal gaming, and its acceptance of the recent liberalization of gambling laws in most US states. The fierceness . . . in this area is puzzling until one realizes the one factor at stake in . . . traditional gambling, but not at stake in Internet gambling: Money . . . Internet gambling, hosted by foreign operators, not only generates zero governmental revenue and zero jobs, it also threatens traditional gambling.[30]

While in the EU a fear of loss of revenue cannot by itself justify restrictions on foreign gambling providers from within the EU (as shown above), is such justification acceptable outside the EU, or is it perhaps a protectionism inconsistent with free trade commitments?

WTO and GATS

This issue is precisely what lay at the heart of the complaint lodged with the WTO by Antigua and Barbuda against the US in 2003. The dispute was first heard by a WTO Dispute Settlement Panel[31] and then, in 2005, by the WTO Appellate Body.[32] The Caribbean State alleged that the US

bookmaking (that is, the acceptance of the bets) occurred in the Dominican Republic and Jamaica where it was legal, rather than in Texas where it was illegal.

[28] *US* v. *American Sports Ltd*, 286 F 3d 641, 653f (2002).

[29] *Ibid*., 660. [30] Hurt, above n. 6, 3f.

[31] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WTO Panel, 10 November 2004, WT/DS285/R).

[32] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WTO Appellate Body, 7 April 2005, WT/DS285/AB/R).

prohibition on the cross-border supply of gambling and betting services was inconsistent with 'market access' commitments made by the US under Article 16 of the General Agreement on Trade in Services (GATS). Antigua blamed, at least partly, the increasingly aggressive US strategy to impede the operation of cross-border gaming activities in Antigua for the significant decline of gambling operators in Antigua: 'from a high of up to 119 licensed operators, employing around 3,000 and accounting for around ten per cent of GDP in 1999, by 2003 the number of operators had declined to 28, employing fewer than 500.'[33]

The opinion of the Appellate Body gave no clear win to either party. It rejected the US claim that, by excluding sporting services from its commitments, it had also excluded gambling and betting services, and affirmed that 'by maintaining the Wire Act, the Travel Act and the Illegal Gambling Business Act, the United States acts inconsistently with its obligations under Art. XVI . . . of the GATS'.[34] Nevertheless, reminiscent of *Gambelli*, the Appellate Body found that these Acts fell within the 'public moral and/or public order' exception[35] upon which States can rely to resurrect market access barriers, and that these Acts were in fact 'necessary' with no alternative measure being 'reasonably available' to the US.[36] Nevertheless, the US had failed to comply with the requirements of this exception, as domestic and foreign providers were not treated the same: the Interstate Horse Racing Act exempted domestic gambling operators from the prohibitions under the above three Acts. In short, similar to *Gambelli*, this case says that you cannot have your cake and eat it: restrictions on offshore gambling providers may be legitimate if based on concerns for public morals or order, but then these restrictions must be applied across the board, including to domestic operators. For this discussion, this case once again shows how vigorously States will defend their domestic interests against foreign online invaders and this is condoned despite free trade commitments as long as the restrictions are not designed to protect the local industry and domestic economic interests, at least not blatantly so.

[33] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WTO Panel, 10 November 2004, WT/DS285/R), para. 3.5.

[34] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WTO Appellate Body, 7 April 2005, WT/DS285/AB/R), para. 265.

[35] Art. 14(a) of the GATS.

[36] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WTO Appellate Body, 7 April 2005, WT/DS285/AB/R), paras. 300ff, in particular para. 326.

Ultimately, the US, like any State relying on the country-of-destination approach, faces problems in enforcing its restrictions or prohibitions against foreign providers, save those rare instances when the perpetrator happens to be on its territory.[37] In an attempt to overcome this problem, the US has focused on intermediaries within their enforcement jurisdiction (that is, on their territory): financial institutions, such as credit card providers, and local advertisers, whether print, broadcast or online outlets, such as Google or Yahoo. Although legislative attempts to criminalise the participation of these intermediaries have so far failed,[38] they have – with the threat of prosecutions under existing law – been bullied into blocking payments, and refusing the sale of advertisements, to offshore gambling providers.[39] Although some of these measures can be circumvented, for example by gambling providers billing punters through other companies to disguise payments as product purchases, the Antiguan complaint to the WTO bears testimony to the fact that the US strategy is paying some dividends.

Australia

Yet another example of the country-of-destination approach can be found in the Australian Interactive Gambling Act 2001 (Cth). It imposes a regime whereby it is an offence to offer gambling services to people in Australia.[40] This does not mean that it is not possible to set up shop in Australia, but simply that those services cannot be offered to Australians. In contrast to the UK, Australia – after an initial period of licensing Internet gambling operators – decided to modernise its law by banning online gambling in respect of Australians. Of course, such a ban could only achieve its desired outcome if the legislation also tackles Internet gambling content hosted outside Australia but *destined* for the Australian market; and it does precisely that. First, the above offence is not limited to Australian gambling suppliers: the Act extends to 'acts, omissions, matters and things outside Australia'.[41] Secondly, the ban on

[37] See e.g. *US* v. *Cohen* 260 F 3d 68 (2d Cir. 2001), discussed in Hurt, above n. 6, 52f.

[38] For example, the Internet Gambling Funding Prohibition Act (108th Congress, 13 March 2003).

[39] Hurt, above n. 6, 53ff.

[40] Sections 8 and 15 of the Interactive Gambling Act 2001 (Cth) and also s.3 (Simplified Outline). *Gambling Review Report*, above n. 8, para. 30.12, seems to suggest that this ban only applies to Australian interactive gambling suppliers, which is not the case.

[41] Section 14 of the Interactive Gambling Act 2001 (Cth). Also compare ss.15 and 15A: pursuant to the former, it is an offence to provide interactive gambling services to customers in Australia; pursuant to the latter, only *Australian-based* interactive gambling services may not be provided to customers in designated countries.

outsiders is 'enforced' (i.e. at least the attempt is made) through imposing certain obligations, such as the provision of Internet content-filtering software on local Internet service providers.[42]

New Zealand

Finally, the New Zealand Gambling Act 2003 also prohibits remote interactive gambling, save minor exceptions.[43] However, New Zealand tackles foreign gambling providers differently than Australia: its prohibition on remote interactive gambling does not apply to 'gambling by a person in New Zealand conducted by a gambling operator located outside New Zealand'.[44] It deals with those operators indirectly by prohibiting foreign gambling services from being promoted, advertised or financed in New Zealand.[45] This prohibition does not apply just to foreign gambling operators (against whom it is difficult to enforce) but also to local intermediaries such as search engines and other sites living off advertising revenue. The idea behind this approach is clearly that, if these foreign gambling sites are not easily known or accessible, then the likelihood of them being used is relatively small and thus prohibiting their use is unnecessary. So, although New Zealand adopts on the face of it a country-of-origin approach to regulating online gambling, it clearly does not leave offshore gambling services unregulated, and seeks to minimise their effect on New Zealand territory by clamping down on their public exposure.

All the above examples again bear testimony to the widespread rejection of the exclusive country-of-origin approach. States are not prepared to sit back and let offshore suppliers of online services infiltrate their territories and do what local suppliers are not allowed to do, nor harm their local population and, more legally controversially, undermine the local industry. And the regulation of online gambling is a prime example of all these concerns which underlie the endorsement of the

[42] See s.3 (Simplified Outline) and Division 3 (Action to be taken in relation to a complaint about prohibited Internet gambling content hosted outside Australia) of the Interactive Gambling Act 2001 (Cth). But note, Responsible Gambling Council (Ontario) 'Law Fails to Slow Online Gambling in Australia' (8 February 2002), *Newscan*, www.responsiblegambling.org/articles/020802_06.pdf.

[43] Sections 9(2)(b) and 19(1)(a) and (c) of the Gambling Act 2003.

[44] Section 4 of the Gambling Act 2003.

[45] See ss.15, 16 and 19(1)(c) to (j) of the Gambling Act 2003 and s.4 for the definitions.

destination-focused approach. All the more surprising then is that the UK has decided to defy that trend.

B. The exclusive country-of-origin approach and its flaws

The UK Gambling Act 2005

In the UK, under the Gambling Act 2005, it is an offence to provide facilities for gambling without an operating licence.[46] For remote gambling – defined as gambling in which persons participate by the use of remote communication such as the Internet, telephone, television or radio[47] – this prohibition applies, by virtue of s.36, 'to the provision of facilities for remote gambling only if at least one piece of remote gambling equipment used in the provision of the facilities is situated in Great Britain'.[48] Such equipment means equipment used to register a punter, to present a person with a game or virtual event for the purpose of gambling, to determine the outcome of the gamble or to store information relating to the result.[49] Importantly, it excludes the computer that is used by the gambler.[50] In other words, the section looks exclusively to the location of the operator, or more accurately its technical equipment. If at least part of its equipment is located in Britain, then the requirement for an operating licence arises. Conversely, an operator with no equipment in Britain can offer its gambling services in the UK without a licence. This approach to regulatory competence is the classic exclusive country-of-origin approach (albeit, as will be seen, one particular version of it): only the State(s) from which the services originate can impose its/their law on the provider. The question is: why does the UK swim upstream and adopt the country-of-origin approach so clearly rejected elsewhere?

The answer to that question cannot be found by searching for the 'true' location of the online activity. There is no such location. The choice between the country-of-origin and the country-of-destination approaches does not come down simply to determining the objective location of the gambling activity, although this appears to be suggested by the UK Department for Culture, Media and Sport:

[46] Section 33(1) and (2) of the Act. [47] Section 4 of the Act.

[48] Section 36(3) of the Act. For a comparable section, see Art. 4 of the Data Protection Directive, 95/46/EC, according to which the data-protection rules provided for by the Directive are applicable only when the controller is either established within the EU or uses equipment situated within the EU in order to process data.

[49] Section 36(4) of the Act. [50] Section 36(5) of the Act.

> the perspective of each state will be shaped by its understanding of where any gambling event is actually taking place ... For example, the US Department of Justice has opined that online wagering takes place simultaneously in both the player's point of origin and the jurisdiction where the gambling operator is based. In Britain we are coming from a different policy angle with the presumption that the regulated activity takes place where the operator is based.[51]

In fact, the opposite is the case: the relative perspective of States on gambling shapes their views as to where the gambling activity should be held to have occurred. The question is: what shapes these perspectives? If the country-of-origin approach avoids the main flaws of the country-of-destination approach (uncertainty, overregulation and enforcement problems[52]), why is it not more popular? What are its flaws and how have these been dealt with, if at all, by the UK? The following evaluates the various flaws of the origin rule, the weight of which varies depending on the activity and legal issue in question.

Loss of economic rewards

Gambling is tolerated and at times encouraged by States because it generates economic activity, employment and tax revenue. States are concerned by offshore operators (and thus seek to restrict them through the destination approach) because foreign providers and their home States reap the economic rewards without 'sharing' it with the State where the activity takes place.[53] That State is left only with the problem gamblers. In *Gambelli*, the defendant alleged that the motives of the

[51] *The Future Regulation of Remote Gambling*, above n. 8, paras. 112f.

[52] Generally, see the discussion in Chapter 4. especially section 2.G. On the whole, the enforcement strategies adopted are costly, impractical and only partially effective. See *Gambling Review Report*, above n. 8, para. 30.6; *The Future Regulation of Remote Gambling*, above n. 8, para. 102, noting that 'in the USA where, despite the apparent illegality of cross border gambling, more of its citizens gamble online than anywhere else in the world'. Recently, the CEO of a gambling company was arrested on entering the US: Jason Gross, 'Internet Gambling and the Law – Prohibition vs. Regulation' (August 2006) *The Metropolitan Corporate Counsel* 2, www.metrocorpcounsel.com/pdf/2006/August/11.pdf; Australia's prohibition also appears to be circumvented regularly: Adam Creed, 'Law Fails to Slow Online Gambling in Australia' (6 February 2002) 4(6) *Newsbyte News Network*.

[53] This concern applies across the board of online commercial activity, but is particularly acute in respect of highly profitable sectors, such as gambling or the sale of drugs. For the latter, see Ayers, above n. 7, 949, 965.

Italian government for the maintenance of the national monopoly were not quite as innocent as claimed:

> The concerns cited by the national authorities relating to the protection of bettors against the risk of fraud, the preservation of public order and reducing both opportunities for gaming in order to avoid the damaging consequences of betting at both individual and social level and the incitement to spend inherent therein are groundless because Italy is increasing the range of betting and gaming available, and even inciting people to engage in such activities by facilitating collection in order to increase tax revenue. The fact that the organising of bets is regulated by financial laws shows that the true motivation of the national authorities is economic.[54]

The UK is not oblivious to these concerns but hopes to achieve more profitable results by turning a vice into a virtue. The UK thinking goes: if foreign gambling operations cannot be effectively controlled,[55] let us make them unattractive, let us become the best and safest gambling haven in the world. The Regulatory Impact Assessment to the Act states:

> There is a potentially vast international market for which gambling operators based in this country will be encouraged to compete and consumers both here and abroad will be able to access a full range of gambling sites licensed and located here, safe in the knowledge that probity and integrity of the gambling operators and products they offer are assured.[56]

The UK approach is premised on the idea that gambling operators – rather than fleeing from British territory to avoid local regulation – will

[54] *Criminal Proceedings against Piergiorgio Gambelli*, Case C-243/01 [2003] ECR I-13031, para. 26; see also para. 38 for the submission of the Portuguese Government: 'Bettors in the small Member States would therefore be financing the social, cultural and sporting budgets of the large Member States and the reduction in revenue from gaming would force governments in the smaller Member States to finance public initiatives of a social nature and other State social, sporting and cultural activities by other means, which would mean an increase in taxes in those Member States and a reduction in taxes in the big States.'

[55] *A Safe Bet for Success*, above n. 8, para. 4.46.

[56] *Draft Gambling Bill – Regulatory Impact Assessment*, above n. 8, para. 6.7; see also paras. 6.13–6.14, and *Gambling Review Report*, above n. 8, paras. 12.14–12.16, and *First Report*, above n. 8, para. 556: 'The Henley Centre predicts that net revenues for the UK from remote gambling sources would rise to £613 million by 2010 with the changes proposed by the draft Bill [i.e. the legalisation of running an online gambling business in the UK].'

adopt it as their home because the commercial benefits of being seen to be properly regulated outweigh the compliance cost. The UK gambling industry will boom with consumers worldwide preferring British providers to unregulated, untrustworthy enterprises from elsewhere.

The hitches with that argument are, first, local operators cannot exploit lucrative foreign markets without coming into conflict with foreign law because, as seen above, these other States do not follow the UK approach. Just because the UK adopts an exclusive country-of-origin approach does not immunise local operators from foreign gambling law. The only providers to gain a regulatory advantage under the UK regime are foreign operators that offer gambling services in the UK.

Secondly, as the above examples amply show, the UK is not the only State to regulate gambling: most Western States make some attempt to protect consumers from exploitative practices. Thus it is doubtful that the UK is the only place that can vouch for the probity and integrity of its gambling industry. For a respectable gambling provider who targets consumers worldwide, it would probably be cheaper to establish itself in some 'regulated' State other than the UK, as UK consumers can be targeted without any extra legal compliance cost. If, on the other hand, the UK market is the primary market, establishment in Britain is probably helpful as local consumers are likely to have greater confidence in locally established providers. But for those providers, the country-of-origin approach offers no extra advantages. In short, it seems at best inconclusive and at worst unlikely that the country-of-origin approach will attract gambling providers to, rather than repel them from, the UK.

Forum-shopping and the race to the bottom

Particularly in the commercial context, an exclusive country-of-origin approach is likely to give rise to, and encourages, forum-shopping.[57] In the absence of any other pressing reason,[58] gambling businesses can minimise regulatory compliance cost (and may indeed have a duty to do so to maximise profits for their shareholders) by moving to the State

[57] Concern expressed e.g. in *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 199. See Hörnle, above n. 2, 115ff, for a discussion of the evasion principle in the EU where the freedoms arising under mutual recognition and the origin rule have triggered some forum-shopping.

[58] One pressing reason in the online context, as argued above, may be that consumer confidence is higher in locally established businesses, with a local offline contact point.

with lenient or no regulatory requirements – comparable to tax havens, flag-of-convenience countries or the Delaware syndrome in respect of company law.[59] In the online context, the movement of data is particularly easy and from the perspective of the consumer at first not noticeable – although it is the consumer who, no doubt, is one of the primary losers of forum-shopping.

So what is wrong with forum-shopping? It has been shown that competition between regulatory regimes fostered by, and in turn fostering, forum-shopping tends to trigger a regulatory race to the bottom: it is not the State with the most well-balanced regulatory regime that will enjoy most popularity, but the most lenient one, the one most favourable to businesses. In the gambling context, that would be States such as Venezuela, Antigua, Grenada and the Cook Islands.[60] The operator can choose the place of origin – often a place with no real link with the activities – motivated by factors in the interests of neither its customers nor the wider public. From a principled angle, forum-shopping is often[61] unsatisfactory as regulatory competence is no longer based on the relative strength of the connection between the activity and the State. And, in terms of States' economic interest, forum-shopping is a serious concern when it undermines local businesses,[62] a matter of not inconsiderable interest in the gambling context, as seen above.

One way to minimise forum-shopping would be to fix the State of origin by reference to a fact that cannot be so easily manipulated and shifted to another place, for example the seat of the management of the

[59] In the company law context, see Simon Deakin, *International and Jurisdictional Issues* (ESRC Centre for Business Research, University of Cambridge, 1999); Simon Deakin, *Legal Diversity and Regulatory Competition: Which Model for Europe*, Working Paper No. 323 (Centre for Business Research, University of Cambridge, 2006), www.cbr.cam.ac.uk/pdf/WP323.pdf.

[60] Wolfgang Fritzemeyer and Regina Rinderle, 'Das Glücksspiel in Internet – Straf- und wettbewerbsrechtliche Verantwortunglichkeiten sowie vertragsrechtliche Rahmenbedingungen' (2003) 8 *Computer und Recht* 599, 599.

[61] For example, in respect of contract law, contractual autonomy means that the parties can shop for the law and court which suits them best, subject to exceptions as discussed in Chapter 3.

[62] The unfair competitive advantage of foreign, more leniently regulated, online businesses underlay both *Deutscher Apothekerverband eV* v. *0800 Doc Morris NV*, Case C-322/01 [2003] ECR I-14887 and *Arzneimittelwerbung im Internet* (BGH, 30 March 2006, I ZR 24/03), see below n. 87. Note, forum-shopping for law, rather than for cheap labour, does not necessarily entail that the main operations of the business are relocated: Deakin (1999), above n. 59, 3f.

enterprise.[63] As the UK Act looks solely to the technical equipment that facilitates the gambling, a local gambling enterprise would not need to move its head offices outside Britain to avoid the licensing requirement; uploading all relevant data onto a server in Antigua would seem enough to do the trick. Whether that is fair and desirable is questionable, but, as argued above, the assumption in the UK appears to be that out of commercial considerations providers would not want to evade regulation.

In this context, it is also noteworthy that the origin principle is not quite as clear-cut and easily ascertainable as its proponents would like one to believe. The more obvious 'origin' alternatives would be the seat of the management of the company, the seat of any of its editorial offices or the place of the server to which the material is eventually uploaded.[64] Even if the latter place is chosen, that does not necessarily solve the problem: 'Matter may be stored on more than one web server, and with different web servers at different times. Different parts of a single web page may be stored on different web servers in different jurisdictions.'[65] There is certainly no universally accepted understanding of the origin principle; what they all have in common is that there is someone or something within the enforcement reach of the State asserting competence. Under the Electronic Commerce Directive, the origin of the online service is determined by reference to where 'a service provider ... pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required ... do not, in themselves, constitute an establishment of the provider.'[66]

While the notion of establishment of the provider seems straightforward, in fact the wording of the section is the end-product of significant

[63] The 'real seat' of an enterprise (rather than the easily manipulated place of incorporation) is used in a number of EU States as the nexus determinative of, for example, the application of domestic company law, Deakin (1999), above n. 59, 5ff, but see *Kamer van Koophandel en Fabrieken voor Amsterdam* v. *Inspire Art. Ltd*, Case C-167/01 [2003] ECR I-10115.

[64] In *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, the editorial office was in New York and the server in New Jersey; see also para. 41 for other possible connections: the location where the material was initially composed or the place of incorporation of the provider. Discussed in Australian Law Reform Commission, *Choice of Law*, Report No. 58 (1992), 57.

[65] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 199.

[66] Art. 2(c) of the Electronic Commerce Directive, 2000/31/EC.

litigation before the European Court of Justice.[67] Be that as it may, the arguments about the ambiguities of the origin rule seem far less problematic than those of the destination approach. Assuming a definition of 'origin' is fixed, the business is in a position to order its affairs accordingly. It knows where it uploads its data or where it has a fixed establishment, can control those locations and would not face any unexpected legal exposure. Yet, would the consumer know this, too?

Shift of regulatory burden

The exclusive country-of-origin approach is haled by online publishers because it minimises their regulatory burden by restricting it to the one, or at most a few, legal regimes. What they do not mention is that, while it would ease their regulatory burden, often that burden would simply be shifted to the online consumer. In the private context, it would mean that the consumer or victim has to bring or defend proceedings in a foreign place determined by reference to foreign law. As prevention is better than cure, online consumers should ascertain the consumer protection provisions applicable in the origin State prior to any transaction. The end-user might also want to guard against the risks of dealing with a discreditable enterprise by finding out about the existence of, and compliance with, licensing requirements and which foreign governmental body, if any, deals with consumer complaints.[68] But first the consumer would have to determine the whereabouts of the business or of its server(s) – depending on which version of the country-of-origin approach is adopted. Any consumer who frequently transacts online business would, theoretically at least, be confronted with a host of foreign legal regimes which affect his dealings. Of course, this is all fancy theory as even the most conscientious and legally adept consumer would be overwhelmed by these legal expectations and safety procedures. The point is that the exclusive country-of-origin approach does not magically reduce the online legal burden *per se* but often just shifts it to the consumer, who tends to be the weaker party. As argued above, the Act is premised on the idea that local consumers will shun foreign providers in favour of respectable local ones.[69] A wise choice.

[67] For the background to the section, see Hörnle, above n. 2, 113; and *Commission* v. *UK*, Case C-222/94 [1996] ECR I-4025, concerning Art. 2(1) of the Television without Frontiers Directive, 89/552/EC (later revised by 97/36/EC).

[68] See, for example, Australian Broadcasting Authority, www.aba.gov.au/about/legislation/gambling.html and www.aba.gov.au/contentreg/complaints/internet/gambling.shtml.

[69] See above n. 56 and the related discussion, and below n. 72.

No protection from harmful foreign content

The potential loss of economic rewards is not the only reason for seeking regulatory oversight over foreign providers through the destination approach. Protecting the local population from harmful foreign content infiltrating the State is another motive. What is considered 'harmful' foreign content varies widely between States, ranging from politically unacceptable content in authoritarian regimes[70] to morally or commercially unacceptable content in Western States. In the gambling context, State action is often explicitly based on the desire for 'the prevention of fraud or the protection of bettors against themselves'.[71] Under the exclusive country-of-origin approach, no such attempt is made. The UK does not seek to protect local gamblers from foreign gambling enterprises. This may be defended on two grounds: first, efforts to exercise control over foreign content are often in any event only partially effective.[72] Secondly, it is a rather paternalistic attitude on the part of the State to shield its population from all undesirable content. In the UK, gamblers are given the free choice between the regulated domestic industry and the unregulated foreign industry and, if they opt for the latter, that is their risk.

This latter argument is less persuasive in the context of other online activities, such as the sale of pharmaceuticals or weapons where State control would seem pivotal to protect the individual or the community.[73] Thus the origin principle would be less acceptable there. The argument also holds less water in respect of children and other vulnerable people who cannot protect themselves. Although it is a bone of

[70] For the position e.g. in China or Cuba, see Shanthi Kalathil and Taylor C. Boas, 'The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution' (2001), Carnegie Endowment Working Papers, Global Policy Program No. 21, www.carnegieendowment.org/files/21KalathilBoas.pdf.

[71] *Criminal Proceedings against Piergiorgio Gambelli*, Case C-243/01 [2003] ECR I-13031, para. 35.

[72] *First Report*, above n. 8, paras. 557 and 559: 'The Government and remote gambling businesses have also noted that, given the global nature of the business, it is not feasible to prevent UK citizens from engaging in remote gambling and that it is, therefore, preferable to have a well-regulated UK-based industry ... Not only could this have significant fiscal advantages but it also recognises the fact that, even if it were desirable, it would be impossible to prohibit the use of remote gambling services by UK citizens effectively.'

[73] For pharmaceuticals see above n. 7 and below n. 87; Moerel, above n. 2, 190, notes the inconsistency between endorsing the origin rule in the EU for the sale of drugs but not for consumer contracts; for weapons see BBC, 'Police Raids on Weapons Website' (4 November 2004), BBC News UK edition, http://news.bbc.co.uk/2/hi/uk_news/england/3985231.stm.

contention whether the Internet makes underage gambling easier than it has previously been,[74] one of the three objectives of the UK Act is to protect 'children and other vulnerable persons from being harmed or exploited by gambling'.[75] How can that be achieved if foreign gambling operators are unregulated? Clearly, for underage surfers, it matters not from where a gambling site originates; they may even steer towards foreign sites when excluded from local sites. The Act creates offences in respect of allowing children or young persons to gamble[76] and expects gambling operators to implement '[s]creening, e.g. to prevent under age play; Reality checks to counter problem gambling; Screen links e.g. to the Gambling Commission and those providing help to problem gamblers; Player identification and verification procedures . . . Training so that staff will be able to identify gambling patterns that may indicate problem gambling and wider social issues.'[77]

And these requirements appear to be applicable to offshore online operations. The Explanatory Notes to the initial Draft Bill stated that 'a person . . . who has no relevant equipment within Great Britain, will not fall within the scope of the *draft Bill or any of its provisions*'.[78] Yet, this interpretation was and is inconsistent with the wording of the sections according to which the at-least-one-piece-of-gambling-equipment-in-the-UK rule (s.36) only applies to the requirement for an operating licence (s.33) and not to the whole Act. This more narrow interpretation appears to be confirmed by the amended Explanatory Notes to the Act.[79] Foreign gambling operators with no equipment in the UK do not enjoy total immunity from all the provisions of the Act: they are subject to the child-protection provisions and must not allow children from the UK to gamble on their sites.[80]

[74] Hurt, above n. 6, 45ff.

[75] Section 1(c) of the Act. On the harmful effects of gambling, see Dee Dee Doke, 'Dicey Plans?' (2005) January *Communitycare* 32, www.communitycare.co.uk.

[76] Part 4, and in particular ss.46 and 48 of the Act.

[77] *Draft Gambling Bill – Regulatory Impact Assessment*, above n. 8, para. 6.22. For these requirements to be taken seriously by the gambling industry, vigilant policing will be necessary. Recently, the Trading Standards Institute conducted a survey and found that many known retailers failed to carry out checks on their online customers' ages in relation to purchases of alcohol, knives or adult videos: David Sanderson, 'Children Buy Weapons Online' (31 October 2005), *The Times*, 27.

[78] *Draft Gambling Bill – Explanatory Notes*, above n. 8, para. 79 (emphasis added); see also *The Future Regulation of Remote Gambling*, above n. 8, para. 113.

[79] *Explanatory Notes to Gambling Act 2005*, above n. 8, para. 138f.

[80] Section 46 of the Act.

In short, as the exclusive country-of-origin approach fails to offer sufficient protection to those most in need of it, the Act introduces for limited purposes the country-of-destination approach after all. But unless those provisions can be enforced against foreign operators, UK regulators may be accused of paying mere lip service to the child-protection objectives. Currently, unlike in Australia, local ISPs are not expected to filter out non-compliant foreign providers.[81] Generally, this backtracking from the origin rule in order to protect children highlights that there are some interests and activities in respect of which the State would be hard pushed to abdicate its regulatory responsibility, quite regardless of the origin of the online activity.

Lowest common denominator

The theoretical implication of the destination rule is that online actors have to comply with the strictest laws of all destination States (the highest common legal denominator) in order to comply with all of them. The origin rule entails the reverse: the legal standards which all States have to accept in respect of any particular type of online activity are those of the origin State with the most lenient regulation. If online content originates in Cloudcuckooland which has no law on gambling or pornography, the origin rule would prevent any other States from regulating it. If US online publishers were subject only to US free-speech standards, stricter speech laws (for example, on defamation or hate speech) by other States would be undermined. The origin rule entails *de facto* legal harmonisation at the lowest level. The simple implication is: the origin rule is only ever acceptable if the lowest common denominator is acceptable. In the UK, foreign online gambling operators are, rightly or wrongly, perceived as non-threatening (apart from their impact on children) based on the strength of the local industry. In the case of the Electronic Commerce Directive, the lowest common denominator is acceptable because it is not that low at all, which provides an essential key to the Directive.

The special case of the Electronic Commerce Directive

The Electronic Commerce Directive (hereinafter, the Directive) provides another rare example of the exclusive country-of-origin

[81] Pursuant to s.5(2)(c) of the Act (but note also s.5(3)), ISPs providing merely access to the Internet will not be considered as providing facilities for gambling and thus are outside the ambit of the Act.

approach:[82] pursuant to Article 3(2) Member States 'may not . . . restrict the freedom to provide information society services from another Member Statess'. The rule applies to any legal requirements within 'the coordinated field', such as legal prerequisites for carrying out the activity or requirements concerning the content or quality of the service.[83] Despite some uncertainty as to what exactly falls within the 'coordinated field',[84] there is no doubt that the rule has 'a very wide scope as it applies across all sectors [bar a few exceptions including gambling] and not just to the areas harmonized by the Directive'.[85]

The almost wholesale incorporation of the country-of-origin approach into the EU online domain can only be properly understood against the history of European integration and the Single Market. A cornerstone within that history has been the principle of mutual recognition and the more specific freedoms such as the free movement of goods and the freedom to provide services inside the internal market.[86] Generally, those freedoms entail that the Member State cannot erect obstacles on incoming goods and services from other Member States. This has not prevented States from being able to apply their laws to foreign goods and services entering their markets. But it has meant that the destination State has to exercise regulatory restraint in respect of them, and treat them not just no more harshly than domestic businesses but even at times more leniently. For example, a Member State may have to forego the requirement for a fixed establishment – which it legitimately imposes on certain domestic businesses – in respect of an equivalent foreign business, thus facilitating the occasional and temporary provision of the service. So EU Member States are well accustomed to compromising their peculiar national laws in the name of an open market.

The origin rule goes a step further than the above freedoms in that it prevents destination States from regulating foreign incoming services altogether, and not just when that regulation would be discriminatory or

[82] Discussed in depth in Hörnle and Moerel, above n. 2. See also UK Department of Trade and Industry, *A Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)* (31 July 2002), paras. 4.3–4.8.

[83] Art. 2(h) of the Directive.

[84] For different views and perceived uncertainties, see e.g. DTI, above n. 82, para. 4.8; Hörnle, above n. 2, 92f; Joakim S. T. Oren, 'International Jurisdiction over Consumer Contracts in e-Europe' (2003) 52 *International and Comparative Law Quarterly* 665, 668.

[85] Hörnle, above n. 2, 92. But note Smith, above n. 2, 532: 'A country of origin solution without derogation for the country of receipt is, in reality, politically feasible only (if at all) if a substantial degree of uniformity ("harmonisation") of national law is achieved.'

[86] Arts. 28 and 49 of the EC Treaty, respectively.

amount to an obstacle.[87] But even that extra step has been taken before in the EU, for example in the Television without Frontiers Directive,[88] where, however, the origin rule is restricted to the areas of law harmonised in it.[89] What is significant is that the origin principle in the Electronic Commerce Directive falls like the above freedoms within the tradition of mutual recognition and the same climate of mutual respect for each other's legal regimes; it is a progression within a well-established tradition.[90]

[87] In respect of the freedom of movement of goods, the ECJ held in *Deutscher Apothekerverband eV* v. *0800 Doc Morris NV*, Case C-322/01 [2003] ECR I-14887, that the requirement under German law that certain drugs must be sold in pharmacies was an unjustified restriction, in this case on the online activities of a Dutch pharmacy. Such a requirement was only justified for prescription drugs. Since then, the Directive has come into force, with the online sale of drugs being within the scope of the 'coordinated fields'. Nevertheless, in *Arzneimittelwerbung im Internet* (BGH, 30 March 2006, I ZR 24/03), paras. 27–30, concerning a Dutch website selling drugs requiring a licence under German law, the *Bundesgerichtshof* held that the origin rule did not extend to the regulation of their delivery; although it extended to advertising drugs online, the destination rule could be justified under one of the exceptions in Art. 3(4)(a)(i): for the protection of public health.

[88] Art. 2a(1) of the Television without Frontiers Directive, 89/552/EEC (revised by 97/36/EC): 'Member States shall ensure freedom of reception and shall not restrict retransmission on their territory of television broadcasts from other Member States.' For proposals to extend certain provisions of the Directive to certain Internet services, see Proposal for a Directive of the European Parliament and of the Council Amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, COM(2005) 646 final; for general background, see www.euractiv.com/en/infosociety/twf-television-frontiers/article-117550. Other Directives that adopt the origin rule are 89/646/EEC, 93/22/EEC, 92/49/EEC and 92/96/EEC.

[89] Art. 2(1) of the Television without Frontiers Directive, 89/552/EEC, establishes the origin rule with respect to 'fields coordinated by this Directive' and then, unlike the Electronic Commerce Directive, provides no extra definition of 'coordinated fields'. In *Konsumentombudsmannen (KO)* v. *De Agostini (Svenska) AB and TV-Shop i Sverige AB (C-35/95 and C-36/95),* Case C-34/95 [1997] ECR I-3843, para. 32, where the European Court of Justice held that misleading advertising did not fall within the field coordinated by the Directive and thus there was no exclusive competence by the origin State.

[90] Having said that, the origin rule remains a sensitive issue and was dropped from the proposed Services Directive. Press Service, European Parliament, *Free Movement of Services: MEPs Take a Big Step Forward* (Strasbourg Plenary, 13–16 February 2006, Debates and Votes). *Amended Proposal for a Directive of the European Parliament and of the Council on Services in the Internal Market*, COM(2006) 160 final. For some of the difficulty of reconciling the open market with a high level of consumer protection, see Gerrit Betlem, 'Cross-Border Private Enforcement of Community Law', in J. A. E. Vervaelde *et al.* (eds.), *Compliance and Enforcement of European Community Law* (The Hague: Kluwer Law International, 1999).

That tradition accommodates and often presupposes some differences in the national laws of Member States, but equally is premised on relatively harmonised legal standards and encourages further harmonisation. Otherwise, it would simply not be acceptable. When the legal differences are too great, as for example in respect of gambling, the origin rule becomes unacceptable.[91] When relatively harmonised standards exist (as they do in respect of the 'coordinated fields' under the Directive[92]), many of the objections against the exclusive country-of-origin approach are resolved. It leaves little room for forum-shopping, States no longer need to fear that their consumers are harmed by unacceptable foreign content, and consumers themselves can be reassured that foreign legal standards are comparable to local ones.

However, harmonisation does not address the concern that the origin rule entails that the destination State loses economic rewards from local activity to foreign businesses. The Directive addresses that fear through reciprocity: because the origin rule is imposed on all Member States, each State is recompensed for losses to foreign providers by gaining unhindered access to foreign markets. In the UK gambling context, there is no such reciprocity to compensate the UK for its generosity towards offshore enterprises.

The safeguards, coupled with the origin approach, do not stop at relative legal harmonisation and reciprocity. The deference to the origin State in the EU also goes hand in hand with an expectation that that State takes its regulatory responsibility in respect of activities originating from their territory seriously. Consistently Art. 3(1) of the Directive imposes an obligation on origin States to regulate: 'Each Member State shall ensure that the information services provided by a service provider established on its territory comply with the national provisions in the Member State in question which fall within the coordinated field.'[93]

[91] See above n. 11. Also, and perhaps more importantly, in respect of gambling, its inclusion within the Directive would have spelled the end of State monopolies that exist in many Member States in respect of various gambling sectors. The freedom of establishment and the freedom to provide services, *prima facie* applicable to gambling services, are more acceptable as they are subject to wider exceptions; see *Criminal Proceedings against Piergiorgio Gambelli*, Case C-243/01 [2003] ECR I-13031, para. 63: 'moral, religious and cultural factors . . . could serve to justify the existence on the part of the national authorities of a margin of appreciation sufficient to enable them to determine what consumer protection and the preservation of public order require.'

[92] Hörnle, above n. 2, 117.

[93] Similarly, Art. 2(1) of the Television without Frontiers Directive, 89/552/EEC, provides: 'Each Member State shall ensure that all television broadcasts transmitted by

If the origin State fails to discharge that duty (which it might be tempted to do where the activity is only directed to the outside[94]), the destination State may request the origin State to fulfil its duty.[95] If the origin State still fails to do so, the destination State is entitled to take measures to restrict the incoming service, but only after notifying both the origin State and the Commission of its intention.[96] The Commission will examine the notified measures as to its legality under Community law and, if judged illegal, ask the destination State to refrain from taking it. Furthermore, the regulatory responsibility of the origin State is reinforced by various possibilities of litigation: 'the destination Member State could bring infringement proceedings under Article 227 of the EC Treaty or it could ask the European Commission to bring proceedings under Article 226 . . . Individuals in the destination Member State may bring proceedings in the Member State of origin . . . if the country of origin fails to extend its regulation'.[97]

The point is that the origin rule in the Electronic Commerce Directive is not the result of a light-hearted decision taken in an experimental spirit. It has significant precedents in the freedoms based on mutual recognition and the origin rule of the Television without Frontiers Directive and other Directives – all inspired by the promises of an open market. It falls against a background of large-scale harmonisation, or at least approximisation, of legal standards. It is accompanied by reciprocal, mutually monitored legal duties that are enforceable by a superior transnational tribunal. In short, it is the result of a history of integration and part of a tightly orchestrated legal regime ensuring reciprocity and the protection of national interests.

Few, if any, of these conditions would be satisfied, or could easily be created, in the international arena. This is why the origin principle is so rare there. If the exclusive country-of-origin approach is unilaterally adopted by a State such as the UK, it amounts to a unilateral concession

broadcasters under its jurisdiction comply with the rules of the system of law applicable to broadcasts intended for the public in that Member State.'

[94] As the activities do not harm locals and the State benefits from the export of such services, it is likely that it would want to encourage them, for example, through lenient legal requirements: *Commission* v. *UK*, Case C-222/94 [1996] ECR I-4025, where it was held that Art. 2 of the Television without Frontiers Directive, 89/552/EEC, entailed that Member States cannot treat non-domestic satellite services by local broadcasters more leniently than those directed at the local market.

[95] Art. 3(4)(b) of the Directive.

[96] Art. 3(4)(b) of the Directive; see also the requirements in Art. 3(4)(a) as to the type of objectives which may justify taking measures against service providers.

[97] Hörnle, above n. 2, 110 (internal marks omitted). See also Arts. 18 and 19 of the Directive.

Country-of-destination approach	Country-of-origin approach
Legal exposure based on the location of the effects/destination of online activity	Legal exposure based on the location of the origins of online activity
EXAMPLES	
Gambling regulation in the Netherlands, Germany, US, Australian, New Zealand	Sections 33 and 36 of the UK Gambling Act 2005; Art. 3(2) of the Electronic Commerce Directive; Art. 2a(1) of the Television without Frontiers Directive; Art. 4 of the Data Protection Directive
ADVANTAGES	
In principle, States retain control over their territory (regulate activity with an effect on their territory)	No or few concurrent assertions of competence
	Simple (easy foreseeability of the relevant legal regimes for businesses)
	Enforceable (based on presence of the actor or the equipment within the territory)
DISADVANTAGES	
Concurrent assertions of competence; overregulation of online publishers	Local law/protections undermined (unless relatively harmonised standards)
Often not enforceable	Forum-shopping (unless relatively harmonised standards)
	Economic rewards reaped by foreign competitors (unless reciprocity)

which understandably most States are not willing to grant, and one has to wonder whether the UK gamble will pay off. This is also why the EU Member States effectively operate a dual set of competence rules: one for offshore online content from Member States and the other for offshore online content from the rest of the world. Nevertheless, there can be no doubt that – when the origin rule, as in the EU online domain, can be implemented within a broad cooperative framework between States – it provides a competence approach superior to the country-of-destination approach. It is clear, minimises concurrent claims and is enforceable. The table summarises the advantages and disadvantages of the approaches.

3. Online gambling: local providers' foreign activities

A. Lack of cooperation in non-harmonised public law

In response to globalisation, States have pushed the boundaries of their regulatory power with the aim of catching extraterritorial activity which affects them. The purpose is entirely legitimate, namely, the retention of control over their respective territories. However, overall these assertions – which are often unenforceable and result in much concurrency and conflicts – are hardly conducive to an effective and clear allocation system. The main problem underlying the need for, as well as the frequent ineffectiveness of, these expansive claims lies in the lack of cooperation between States. Such cooperation is virtually non-existent in respect of those fields of public law where there are different views as to the general wickedness of the behaviour concerned. A typical example is gambling, where attitudes vary widely, ranging from positive encouragement, to toleration, to outright prohibition. But it is precisely in these non-harmonised areas of law that cooperation is needed most, if States want to protect their peculiar national laws effectively. In respect of activity where the law is relatively harmonised, such as, in the online context, hacking or child pornography, cooperation between States may be useful but is not critical. A State can on the whole be assured that the online activity which causes harm on its territory is also considered harmful, and would be prosecuted, in the place from where it originates. Thus, effectively, in harmonised areas, each State, by enforcing its own law, also enforces foreign laws. However, States cannot rely on such foreign enforcement where the foreign State does not criminalise the behaviour in question. It is in these areas that mutual cooperation could make a substantial difference. The following briefly examines the different options for cooperation, ultimately to highlight its non-existence outside harmonised legal fields.

First, the right to regulate actors and activities within a State's competence does not generally entail a corresponding regulatory responsibility towards other States. Just because activity emanating from one State affects another State, does not mean that the former State is under any duty to restrain that activity to protect the interest of the latter State. Such a duty would give rise to some difficulties,[98] if it would require

[98] In the international arena, a duty comparable to Art. 3(1) of the Electronic Commerce Directive, 2000/31/EC (to regulate the local activity according to the State's domestic laws) would be insufficient to protect the interests of other States with possibly very

more than simply imposing an obligation to restrict the extraterritorial effect of local activity.[99] Certainly, under international law, States are under no obligation to do anything. The foundational principle of non-intervention forbids one State to interfere in the internal affairs of another State,[100] but is limited to acts of the State or attributable or imputable to the State and does not extend to acts by private individuals which have an effect in the territory of another state.[101] Such conduct by private individuals does not give rise to any State responsibility. However, although there is no general State duty to exercise control over local actors or activities, there are some specific duties in specific circumstances. For example, in respect of environmental harms, 'no state has the right to permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another'.[102] Also, quite a few treaties impose on parties the duty to 'prosecute or extradite' persons within their control and alleged to have committed offences covered by the treaty.[103] Finally, arguably even under customary

different views on the subject-matter. By the same token, given the widespread effect of much activity, online and offline, a responsibility on States to deal with those effects in light of specific foreign law would be highly burdensome: Michael Akehurst, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145, 220, where the author discusses difficulties that would arise if States had a duty to apply foreign private law.

[99] This is in fact the approach taken in the s.44 of the Act.

[100] Art. 8 of the Montevideo Convention on Rights and Duties of States (1933) or Art. 3 of the International Law Commission's Draft Declaration of the Rights and Duties of States (1949); Helmut Steinberger, 'Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 397, 413: 'this rule prohibits a State from engaging in *public* acts on the territory of another' (emphasis added). Ian Brownlie, *Principles of Public International Law* (6th edn, Oxford: Oxford University Press, 2003), 290.

[101] Arts. 5–11 of the International Law Commission Draft Articles on State Responsibility. In *Rainbow Warrior (New Zealand* v. *France)*, 74 ILR 241, the offending acts were committed by agents of the French intelligence service and were therefore attributable to France.

[102] *Trail Smelter Arbitration (United States of America* v. *Canada)* (1938) 3 RIAA 1905, 1965. Now reinforced in a number of environmental law treaties, discussed in Rosemary Rayfuse, 'International Environmental Law', in Sam Blay, Ryszard Piotrowicz and B. Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005), 352, 358ff. To what extent this ruling should be restricted to environmental damage would seem a pertinent question in the context of online activity.

[103] For example, Art. 10 of the International Convention for the Suppression of the Financing of Terrorism (1999): 'The State Party in the territory in which the alleged offender is present shall ... if it does not extradite that person, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without undue delay to its competent authorities for the purpose of prosecution.'

international law, States have a duty to assume jurisdiction in respect of some crimes, for example crimes against humanity or war crimes. That duty arises under the universality principle which does not just entitle, but, some argue, obliges, States to exercise regulatory control.[104] By definition, the universality principle only applies to certain heinous crimes which are *universally* condemned. The critical point with these specific regulatory duties on States is that they relate to acts in respect of which there is an international consensus. Also, the relevant activity is very limited in scope. When it comes to the vast majority of regulated or criminalised activity, enshrined only in national law, States are alone.

Secondly, cooperation also comes in the form of extradition, which dates back at least to the middle of the nineteenth century. Yet then and still today, and whether or not based on a treaty, a prerequisite for extradition has been the rule of double criminality:[105] the offence with which the person is charged must be substantially the same in both States. In other words, cooperation depends on the States involved having harmonised views as to the criminality of the activity in question. While such harmonised views are not essential for mutual assistance in the investigation and prosecution of criminal offences,[106] nevertheless the duty to assist tends to be provided for in the context of treaties harmonising criminal law amongst States, such as the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) or, more recently, the Council of Europe Cybercrime Convention (2001).[107] So cooperation is again clearly tied to a consensus as to the criminality of the activities. In all of these cooperative arrangements between States,

[104] Again either 'prosecute or extradite'; argued e.g. by Theodor Meron, *Human Rights and Humanitarian Norms as Customary Law* (Oxford: Oxford University Press, 1989), 210. See also Claus Kress, 'Universal Jurisdiction over International Crimes and the Institut de Droit international' (2006) 4 *Journal of International Criminal Justice* 561, 574, noting the 'verbal' state practice to the effect that crimes against humanity and war crimes must not go unpunished. See also Principle 8 of the Princeton Principles on Universal Jurisdiction (2001), www.princeton.edu/~lapa/unive_jur.pdf, which assumes that the State with universal jurisdiction has a duty to either prosecute or extradite.

[105] See the discussion by Ivan Shearer, 'Jurisdiction', in Sam Blay, Ryszard Piotrowicz and B. Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005), 154, 168.

[106] See Crime (International Cooperation) Act 2003. Note for mutual assistance there is generally no requirement for 'dual criminality'. See also UK Home Office, *Mutual Legal Assistance Guidelines: Obtaining Assistance in the UK and Overseas* (2nd edn, December 2004).

[107] Chapter III of the Convention. The Convention entered into force on 1 July 2004.

cooperation never extends to enforcing the criminal law of another State. At best, the requesting State is put in a position where it can enforce its own criminal law. But the motive for cooperating is likely to be self-interest.[108] The cooperating State benefits, first, by seeing activities which it itself condemns penalised, and, secondly, when the situation occurs in the reverse by the reciprocal duty owed by the other State.

These forms of cooperation provide no inroad into the general and deeply entrenched rule that a State will never apply foreign criminal or public law or enforce a foreign criminal or public law judgment.[109] Sometimes it is even asserted (although wrongly[110]) that States have no right to do so. This rule of non-cooperation is so deeply entrenched that it has survived significant challenges in the form of increasing globalisation of crimes such as tax evasion, money laundering and fraud, which has not infrequently meant that all State actors involved lost out.[111]

Against this background of general uncooperativeness concerning non-harmonised legal standards, let us return to the UK Gambling Act 2005 and the issue as to how the UK approaches local gambling operators who offer their online services abroad.

B. The UK and Australia: good neighbours

While the UK Act is generous in respect of foreign operators affecting local territory, how does it deal with local operators affecting foreign

[108] Antonio Cassese, *International Law* (Oxford: Oxford University Press, 2001), 13: 'The international community has long been characterized by a horizontal structure and the lack of strong political, ideological, and economic links between its members . . . These features have resulted in the tendency for every State to be self-seeking. Self-interest has held sway.'

[109] Lawrence Collins (ed.), *Dicey and Morris on Conflict of Laws (*13th edn, London: Sweet & Maxwell, 2000), Vol. 1, 89; cf. the position in respect of private law/judgments. See also Philip J. McConnaughay, 'Reviving the "Public Law Taboo" in the International Conflicts of Law' (1999) 35 *Stanford Journal of International Law* 255. This is not to say that there have not been significant developments on the cooperation front, especially in the EU, which are chipping away at the traditional 'public law' taboo; for the initiatives of the European Commission, see http://ec.europa.eu/justice_home/fsj/criminal/fsj_criminal_intro_en.htm; also Convention on Mutual Assistance in Criminal Matters between Member States of the European Union (2000).

[110] Further discussed in Chapter 6.

[111] It has been harmful to States collectively: A. R. Albrecht, 'The Enforcement of Taxation under International Law' (1953) 30 *British Yearbook of International Law* 454, where the author argues against the non-enforcement rule at least in respect of taxation.

territory? While Britain has warmed to the idea of gambling or, as perhaps cynics may say, to the promise of riches, other States have resisted. So it comes as no surprise that the Act has been met with objections, for example, from Scandinavian States[112] which are concerned that their citizens can access UK-based gambling sites and thus easily evade local restrictions. Perhaps in response to these concerns, the Act stipulates in s.44: 'A person commits an offence if he does anything in Great Britain, or uses remote gambling equipment situated in Great Britain, for the purpose of inviting or enabling a person in a prohibited territory to participate in remote gambling.' A territory is a prohibited territory once the Secretary of State has made an order to that effect.[113] Section 44 has a predecessor in the Australian Interactive Gambling Act 2001 (Cth), which makes it an offence intentionally to provide an Australian-based interactive gambling service to a customer in a foreign country which the Minister has declared a designated country.[114] In many ways, both of these provisions seem the rather obvious and natural answer to the difficulties States face in respect of foreign online activity. Yet, in fact, they break with an entrenched tradition of mutual uncooperativeness in respect of their public or criminal law. The UK and Australia say they boldly go where no man has gone before: they offer to help. Why? Certainly, cooperation would entail the loss of profitable foreign markets.

What, if anything, can either State gain by being cooperative? On the whole, States have made their cooperativeness dependent on reciprocity. International treaties providing for regulatory duties, extradition and mutual assistance in the investigation of crimes ensure that all parties to the treaty receive something in return for their cooperation: the cooperation of the other parties.[115] Such reciprocity would be a theoretical possibility, even in the absence of harmonised standards, along the lines of Lessig's suggestion in *Code and other Laws of Cyberspace*:

> Each state has its own stake in controlling behaviors, and these behaviors are different. But the key is this: the same architecture that enables Minnesota to achieve its regulatory end can also help other states achieve their regulatory ends. And this can initiate a kind of quid pro quo

[112] *First Report*, above n. 8, para. 580. [113] Section 44(2) of the Act.
[114] Section 15A of the Interactive Gambling Act 2001 (Cth), also ss.9A and 9B. Note, in a parliamentary hearing, s.15A was specifically referred to as a 'Good Neighbour Clause'.
[115] See Akehurst, above n. 98, 236f, noting that in the US reciprocity has been rejected as a precondition for the enforcement of foreign private judgments.

> between jurisdictions. The pact would look like this. Each state would promise to enforce on servers within its jurisdiction the regulations of other states for citizens from those other states, in exchange for having its own regulations enforced in other jurisdictions. New York would require that servers within New York keep Minnesotans away from New York gambling servers, in exchange for Minnesota keeping New York citizens away from privacy-exploiting servers . . . Each state would enforce a set of regulations for the other states, in exchange for the others states enforcing its own set of regulations.[116]

Lessig suggests that States can help each other in upholding their varying standards by ensuring that those within their territory do not infringe the laws of other States. Despite the obvious attractions of Lessig's proposal (at least from the perspective of regulators), the fact remains that there is absolutely no precedent for such behaviour by States. In respect of public law, they have been willing to swap favours only in respect of harmonised legal fields. In any event, neither the UK nor Australian legislation envisages reciprocity.

What is most noteworthy about both good-neighbour clauses is that they come close to enforcing foreign criminal law. Of course, in both cases the offence itself is created under the respective domestic law but, especially in the UK, the ban on the provision of gambling services to prohibited territories has no domestic equivalent and indeed creates a regime stricter than in the domestic market. Australia, on the other hand, could be accused of hypocrisy if it allowed local gambling operators to flout foreign prohibitions on offering gambling services when such services cannot be legally provided to Australians. So in Australia the good-neighbour clause allows the legal position in respect of the foreign effect of local activity to be aligned with the legal position as it applies domestically. Certainly, both the UK and Australia would have to bear the cost of prosecuting the offence, and the foreign State would be the only clear beneficiary of such prosecutions. These clauses are indeed the work of very selfless neighbours.

[116] Lawrence Lessig, *Code and other Laws of Cyberspace* (New York: Basic Books, 1999), 55. Lessig's idea might have provided the impetus for this clause: see the *First Report*, above n. 8, para. 584, citing a strikingly similar example to Lessig's. Evaluated by Paul Schiff Berman, 'The Globalization of Jurisdiction' (2002) 151 *University of Pennsylvania Law Review* 311, 387ff, where the author expresses doubts about the feasibility of the proposal based on fundamental objections by governments and the costs for businesses, quite apart from the undesirability of zoning the Internet.

But how real are these clauses? Perhaps not that real. To start with there are the statements in the UK Government's position paper, such as:

> If other jurisdictions wish to prevent their citizens from gambling with British based operators then that of course is open to them. There are numerous mechanisms that they might be able to use ... For the gambling operators this will mean that there is no 'black list' of countries from where they are unable to accept customers.[117]

Yet, of course, the cost, impracticality and poor effectiveness of these measures are some of the very reasons why the UK plans not to go down that route. Furthermore, when Lord McIntosh, the Parliamentary Under-Secretary of State, was asked whether the Government intended to use this power (and one may ask why else would it be included in the Act), he responded:

> Not at the moment, no. This is a reserve power which will give us leeway to act if necessary. Let me give you a hypothetical example. In Utah no gambling is allowed at all, no citizen of Utah is allowed to gamble there or anywhere else, according to Utah law. Unless we were lent on very heavily by the United States federal authorities and/or the state of Utah I think we would be very reluctant to declare them to be a prohibited territory. *It is their problem, not ours.*[118]

This attitude is much more consistent with the traditional attitude of States in respect of cooperation. It is insightful, too, that Australia, having had some time to use its good-neighbour clause, has so far failed to nominate any country as a 'designated country', although Denmark appears to have requested such status.[119] Ultimately, it is unlikely that s.44 of the UK Gambling Act 2005 and s.15A of the Australian Interactive Gambling Act 2001 (Cth) are going to break with tradition and amount to anything more than a gesture of goodwill. Nevertheless, both sections are promising, simply by moving away from an understanding of regulatory competence as power only, rather than as power and responsibility.

[117] *The Future Regulation of Gambling*, above n. 8, para. 106, also paras. 106–8.

[118] *First Report*, above n. 8, para. 584 (emphasis added); the Report then goes on to stress that any order by the Secretary of State would have to be approved by both Houses of Parliament.

[119] At least according to Responsible Gambling Council (Ontario), 'Denmark Rejects Australian Online Gambling' (16 May 2003), *Newscan*, www.responsiblegambling.org/articles/Denmark_Rejects_ Australian_Online_Gambling.pdf.

4. An example to follow?

Gambling regulation provides an archetypal example for the challenges faced by States in respect of transnational online activity and particularly in respect of non-harmonised legal areas. The global nature of the Internet means that a State's public policies can no longer be neatly translated into domestic laws without any regard to the policies of other States.

With the Gambling Act 2005 the UK parts with conventional wisdom and behaves like a model world citizen: it treats foreign offshore providers generously (trying not to step on the jurisdictional feet of other States) and is potentially strict with local providers and their behaviour abroad (again trying to minimise conflict with foreign rules and policies). More specifically, in respect of foreign operators, the UK does not go down the destination approach favoured by most Western States that seek to uphold tight restrictions on gambling on their territories. The UK regulatory strategy is both ambitious and moderate. It is moderate in not seeking to control all online gambling services offered in Britain, but merely those which are based in the UK. It is ambitious in that this moderate regulation is ultimately designed to create a more manageable and safer gambling environment than might result from tight restrictions. In that sense, the regulatory approach bears similarities to the legalisation of prostitution or cannabis. Similarly, with respect to local operators and their behaviour abroad, the Act also ventures into new territory by expressly showing respect for the possibly conflicting public policies of other States. This is laudable and perhaps signals the dawn of a new era of cooperation between States in respect of their non-harmonised public laws. It would certainly help States to preserve them in spite of the Internet. The indications so far are not promising.

The more general question is whether other States will or should follow the UK example, in gambling or otherwise, and adopt the exclusive country-of-origin approach. The answer is that the origin approach will remain exceptional. It will be reserved to those areas of online activity where States are comfortable with tolerating foreign content regardless of its probity. Alternatively, as the Electronic Commerce Directive shows, it may make an appearance amongst relatively homogeneous States where one State can place trust in the legal regimes of the other States, and thus is comfortable in foregoing competence in their favour, and where States are willing to cooperate with each other. For

the origin rule to work (and outshine the destination approach as an allocation rule) there has to be a cooperative spirit amongst States going beyond the narrow range of currently harmonised legal areas. There has to be cooperation with tolerance for each other's differences. Such tolerance is currently entirely absent in respect of public or criminal law. The question is: why? That is explored in the following chapter.

6

The lack of enforcement power: a curse or a blessing?

1. Limited enforcement power: a blessing in disguise

If States could enforce all the regulatory claims they assert they have a right in principle to make, the Internet as we know it would not exist. Perhaps we would be left with State-Wide-Webs with the occasional foreign website straying into it. For all but a few multinational companies, it would be far too risky to allow one's site to be accessed outside one's home State. In most European States, there would be no spam, a little controlled pornography, no hate speech sites, no weapons sites, no how-to-build-your-own-nuclear-bomb sites and only the occasional respectable gambling site. There would be few dodgy dealers; scams would be rare; Google would return hundreds instead of millions of results on any search; sites could be approved, and perhaps would be; they would be listed, classified and catalogued in directories. There would be no chaos, but order, not an absolute order but an order like the one we are accustomed to in the real world. Yet, what a dull place it would be. How less rich, informative, convenient and entertaining, how less creative, energetic and dramatic, how less democratic and egalitarian, a place it would be.

Whatever is said below about enforcement, on the need for effective mechanisms, on the shortcomings of current measures in the online world and on possible solutions, comes with a health warning, the warning that a perfectly ordered online world would not be so perfect after all. The discussion reflects a lawyer's perspective or the perspective of regulators who strive for law and order, and for control. The views must be understood against the certainty that the Internet will, at least in the near future, remain an unruly, disorderly and recalcitrant animal, not easily amenable to the tight clutches of State control. It is safe to decry the current legal *status quo* when we know that much of what we ask for will remain beyond our reach. And with that reassurance let us begin, and end.

The discussion has its starting point in the fundamental, universally accepted principle that States are not allowed to engage 'in public acts on the territory of another State without the latter's permission'.[1] A 'public act' is one which is 'by its nature, an act which only the officials of the local State are entitled to perform, as opposed to an act which private individuals may perform'.[2] This means that no State, its organs or individuals acting on its behalf can engage in any act to enforce its laws on the territory of another State: enforcement power is strictly territorial. Whatever regulatory claims States make in principle over online activity originating outside their territory, enforcement jurisdiction imposes tight limits on what States may do to force their regulatory will onto foreign wrongdoers. Lombois' colourful statement captures this: 'The law may very well decide to cast its shadow beyond its borders; the judge may well have a voice so loud that, speaking in his house, his condemnations are heard outside; the reach of the police officer is only as long as his arm . . . he is a constable only at home.'[3] And that applies to all States and all legal areas.

The discussion concerns the implication of this very limited enforcement jurisdiction in the online world – a topic which so far has been relatively neglected in the academic literature.[4] Questions which will be

[1] Helmut Steinberger, 'Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 397, 413; *The Case of the SS 'Lotus' (France* v. *Turkey)* (1927) PCIJ Reports, Series A, No. 10, 18; *Island of Palmas (The Netherlands* v. *United States of America)* (1928) 2 Reports of International Arbitral Awards 829, 838.

[2] Michael Akehurst, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145, 146f. See also F. A. Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recueil des Cours* 1, 13f, Ch. 4, reproduced in F. A. Mann, *Studies in International Law* (Oxford: Clarendon Press, 1973); F. A. Mann, 'The Doctrine of International Jurisdiction Revisited After Twenty Years' (1984) 186 *Recueil des Cours* 9, Ch. 2, 3. For further relevant reading by Mann, see F. A. Mann, 'Conflict of Laws and Public Law' (1971) 132 *Recueil des Cours* 107; F. A. Mann, *Further Studies in International Law* (Oxford: Clarendon Press, 1990). A classic example of a violation of the rule is the entry of government agents into a foreign State to kidnap suspected criminals and bring them to trial, as for example at the heart of the US Supreme Court decision in *Sosa* v. *Alvarez-Machain*, 542 US 692 (2004).

[3] Claude Lombois, *Droit Penal International* (2nd edn, Paris: Dalloz, 1979), 536, cited in Pierre Trudel, 'Jurisdiction over the Internet: A Canadian Perspective' (1998) 32 *International Lawyer* 1027, 1047.

[4] The problem of enforcement is frequently mentioned, but rarely moves centre-stage, in the discussions on competence over online activity: David R. Johnson and David Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367; Henry H. Perritt, 'Will the Judgment-Proof Own Cyberspace?' (1998) 32 *International Lawyer* 1121; Peter P. Swire, 'Of Elephants, Mice, and Privacy: International Choice of

considered are: how has enforcement jurisdiction, or the lack thereof, affected national law as well as the rules of regulatory competence and their underlying assumptions? How have States worked around the territorial restriction either unilaterally or cooperatively? Why are States so reluctant to cooperate with each other? It is one thing to say that no State can engage in public acts on the territory of another; it is quite another matter for States to refuse to cooperate voluntarily with each other when such cooperation would be mutually beneficial. It certainly would help States to retain control over their respective territories in face of the Internet and globalisation more generally. And yet in public-law matters such cooperation only ever occurs at the margins.[5] What is the key to the private-law versus public-law dichotomy that can explain the uncooperativeness in respect of the latter? And what, if anything, does this all mean for the future of online governance?

In this chapter, the regulation of hate speech, or, more specifically, the Yahoo saga, provides the legal context for the arguments.[6] The saga started in 2000 when the Tribunal de Grande Instance in Paris handed

Law and the Internet' (1998) 32 *International Lawyer* 991; American Bar Association (ABA), 'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf; Karsten Bremer, *Strafbare Internet-Inhalte in International Hinsicht – Ist der Nationalstaat wirklich überholt?* (Frankfurt a. M.: Peter Lang Verlag, 2001), http://ub-dok.uni-trier.de/diss/diss60/20000927/20000927.pdf. The Internet exacerbates enforcement problems also for other reasons, e.g. the anonymity of online actors makes identification of wrongdoers difficult; digital evidence is transient; and offensive material can be easily moved to other sites: Graham J. H. Smith (ed.), *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002), Ch. 6.

[5] In the public-law context, there is not-insubstantial cooperation between States in the form of extradition, mutual assistance in the investigation of criminal matters and the transfers of prisoners to their home States. For recent 'online' examples of cooperation, see Arts. 23–35 of the Council of Europe Cybercrime Convention (2001) and Art. 10 of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000). But most of the cooperation is either made specifically dependent on relatively harmonised regulatory views or, in the case of mutual assistance, tends to come as part of a package of legal harmonisation.

[6] There is an enormous amount of secondary literature on the case: Robert Corn-Revere, *Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?*, Briefing Paper No. 71 (2002), Cato Institute, www.cato.org/pubs/briefs/bp71.pdf; Uta Kohl, 'Yahoo! – But No Hooray! for the International Online Community' (2001) 75 *Australian Law Journal* 411; Mathias Reiman, 'Introduction: The *Yahoo!* Case and Conflict of Laws in the Cyberage' (2003) 24 *Michigan Journal of International Law* 663; Horatia Muir Watt, 'Yahoo! Cyber-Collision of Cultures: Who Regulates?' (2003) 24 *Michigan Journal of International Law* 673; Molly S. Van Houweling, 'Enforcement of Foreign Judgments, the First Amendment, and Internet

down a judgment (hereinafter, Yahoo) in favour of the plaintiffs, two French anti-racist organisations, LICRA and UEJF (hereinafter, LICRA) which had sued Yahoo! Inc., a US corporation, and its French subsidiary for allowing surfers from France to buy Nazi artefacts via Yahoo websites.[7] The Paris court found that Yahoo! Inc. had committed 'a manifestly illegal disturbance' (comparable to a nuisance) under the French New Code of Civil Procedure,[8] which in turn was based on the French Criminal Code and the offence of distributing Nazi memorabilia. The court rejected all Yahoo! Inc.'s arguments against the court's competence: that the yahoo.com site was located on a server in California, that it was intended for an American audience or that Yahoo! Inc. could not easily identify and exclude surfers from France from its site.[9] Harm was suffered on French territory, and that was it. Yahoo! Inc. was ordered to prevent access from French territory to the artefacts and hate speech sites in question, backed by a penalty of 100,000 francs per day for non-compliance.[10] In light of subsequent decisions from across the globe, this holding is now hardly extraordinary, and is of no further interest here. The focus here is on the litigation which ensued in the US courts following the Paris judgment. This litigation culminated in a judgment by the US Court of Appeals for the Ninth Circuit (hereinafter, *Yahoo*)[11]

Speech: Notes for the Next Yahoo! v. LICRA' (2003) 24 *Michigan Journal of International Law* 697; Mark F. Kightlinger, 'A Solution to the *Yahoo!* Problem? The EC E-Commerce Directive as a Model for International Cooperation on Internet Choice of Law' (2003) 24 *Michigan Journal of International Law* 719.

[7] *LICRA* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000), affirmed in *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000), www.foruminternet.org/actualites/lire.phtml?id=273/.

[8] Arts. 808 and 809 of the New Code of Civil Procedure.

[9] The court ordered an inquiry into the feasibility of its order, which confirmed its feasibility: *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 11 August 2000).

[10] There is some discrepancy in the penalty between the May judgment (100,000 euros) and the November judgment (100,000 francs). There were also orders against Yahoo! France to remove 'negationist' index headings and links to 'negationist' sites as well as to post a warning on fr.yahoo.com to any users that viewing 'negationist' websites is illegal and subject to penalties under French legislation. The litigation against Yahoo! France is not further considered.

[11] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199 (9th Cir. 2006); reversing *Yahoo! Inc.* v. *LICRA and UEJF*, 145 F Supp 2d 1168 (ND Cal. 2001) (finding in favour of personal jurisdiction); *Yahoo! Inc.* v. *LICRA and UEJF*, 169 F Supp 2d 1181 (ND Cal. 2001) (finding in favour of ripeness of the suit, and the unenforceability of the French order based on the First Amendment); *Yahoo! Inc.* v. *LICRA and UEJF*, 379 F 3d 1120 (9th Cir.

in early 2006. At the heart of that litigation lay the issue of the enforceability of foreign laws and judgments.

The US *Yahoo* litigation provides a particularly apt example for the issues under consideration here. To start with, it concerns a clash of fundamental values between two Western industrialised nations. Unlike the gambling context (see the previous chapter), it is not, first and foremost, the financial interests of the State which are at stake here,[12] but rather moral values embedded deeply within each national consciousness.[13] In terms of cooperativeness, this means that 'all' that is needed is tolerance for another State's values, but is that tolerance forthcoming? Secondly, the initial French litigation cannot easily be characterised as private or public. It occupies the grey middle ground, and therefore raises interesting matters concerning categorisation and the rationale underlying the distinction between public and private law for competence purposes. Thirdly, although the US litigation concerns the enforceability of the French order, in fact ultimately Yahoo! Inc. lost because enforceability in principle, rather than enforceability in the actual case, is what really mattered to the parties. Not unlike in the defamation cases discussed in Chapter 4, actual enforcement of the Paris orders was very much a secondary concern. And this says much about the relative importance or unimportance of enforceability, examined now.

2. Enforceability and legal compliance

A. Enforceability, not enforcement, matters

To start with, questions of enforcement have played a role within two significant jurisprudential debates of long standing. Enforceability has been critical to the debate about when a law is a law properly so called. Are sanctions a necessary element of law, or conversely can there be law in the absence of sanctions? The answers have varied depending on the views one takes on the origins of law and from where it derives its

2004) (personal jurisdiction finding reversed). The US Supreme Court declined to hear an appeal on 30 May 2006: *LICRA* v. *Yahoo! Inc.*, 126 S.Ct 2332 (Mem) (2006).

[12] This is not to say that the outcome of the case does not also have financial implications for online businesses in terms of measures they would have to adopt to ensure compliance with the foreign law.

[13] Another classic instance of such morally or culturally motivated action would be the attempted prosecution in France in 1997 of the website of the French campus of a US institute under French language purity laws: Michael S. Rothman, 'It's a Small World After All: Personal Jurisdiction, the Internet and the Global Marketplace' (1999) 23 *Maryland Journal of International Law and Trade* 127, 131f.

normative force.[14] Another debate on enforceability relates to the efficacy of law and whether sanctions or the threat of them are necessary for a rule of law to be obeyed more often than not:[15] 'Whether or not men do actually behave in a manner to avoid the sanction threatened by the legal norm, and whether or not the sanction is actually carried out in case its conditions are fulfilled, are issues concerning the efficacy of the law.'[16]

This debate relates to the motivations as to why people obey the law and whether a law's enforceability is a critical motivating factor. The discussion here does not revisit either of these debates, but is in substance concerned with the latter: can the efficacy of State law be ensured when its enforceability is severely circumscribed in respect of cross-border online activity? The answer given to that question is consistent with the following broad propositions which emerge from the jurisprudential wrangling about the relationship between the enforceability of law and its efficacy, despite a general lack of consensus on more particular issues:[17] first, as a matter of fact, law has almost always gone hand in hand with coercion – acknowledged even by jurists who hold that sanctions are not a logically necessary ingredient of law.[18] Secondly, the threat of sanctions furnishes one motivating factor for obedience,[19] but there are other important factors inducing compliance or behaviour consistent with the legal norm.[20]

[14] For classical positivists, the enforceability of law is a necessary ingredient of a law properly so called, unlike, for example, for theorists of natural law.

[15] H. L. A. Hart, *The Concept of Law* (2nd edn, Oxford: Clarendon Press, 1994), 103.

[16] Hans Kelsen, *General Theory of Law and State* (Cambridge, MA: Harvard University Press, 1946), 30, see also 39: 'Efficacy of law means that men actually behave as, according to the legal norms, they ought to behave, that the norms are actually applied and obeyed.'

[17] *Ibid*., 17: 'We do not know exactly what motives induce men to comply with the rules of law. No positive legal order has ever been investigated in a satisfactory scientific manner with a view to answering this question . . . All we can do is to make more or less plausible conjectures.'

[18] Neil MacCormick, *Legal Right and Social Democracy: Essays in Legal and Political Philosophy* (Oxford: Oxford University Press, 1982), 232ff; A. L. Goodhart, *English Law and the Moral Law* (London: Stevens & Sons, 1953), 17.

[19] Even a positivist like Austin does not seem to attribute legal compliance solely to the deterrent effect of sanctions, but also to what he refers to as the 'habit of obedience'. Hart, above n. 15, 197ff.

[20] Kelsen above n. 16, 24: 'In all probability, however, the motives of lawful behavior are by no means only the fear of legal sanctions or even the belief in the binding force of the legal rules. When the moral and religious ideas of an individual run parallel to the legal

It is enforceability that really matters, not actual enforcement. The US *Yahoo* litigation illustrates the importance of enforceability of law in the traditional sense, i.e. the threat of a State sanction being applied in case of non-compliance. But, as will be seen, at least in the transnational context, the reason for its importance lies often not simply, or even mainly, in inducing a fear of a sanction in the case of non-compliance, but rather in affirming the foreign law's legitimacy.

In *Yahoo*, the Ninth Circuit heard an appeal against the decision by the District Court for the Northern District of California, in which Yahoo! Inc. had sought a declaration that the French order was unenforceable in the US. This declaration had been granted by the District Court following findings, first, that it had personal jurisdiction over LICRA[21] and, secondly, that the suit was ripe and that enforcement of the French order would be inconsistent with the First Amendment to the US Constitution.[22] However, LICRA emerged from the Ninth Circuit as the winner, even if only by the skin of its teeth. The full bench of the Ninth Circuit delivered a highly divided judgment with three separate decisions; a majority found in favour of personal jurisdiction and a majority of that majority in favour of ripeness but on a count of the overall votes there was a majority of six votes to five in favour of dismissal.[23]

In the end, Yahoo! Inc. lost because its case was too hypothetical:[24] Yahoo! Inc. wanted a decision on enforceability in principle when actual enforcement was not on LICRA's agenda. Yahoo! Inc. wanted a decision on enforceability because that is what really mattered; but it came up against the reluctance of common law courts to pass judgements in the absence of a real dispute. LICRA's victory consisted not in a decision for the

order to which he is subject, his lawful behavior is often due to those moral and religious ideas . . . A man fulfils his legal duty to pay his debts very often not because he wishes to avoid the sanction provided by the law against an individual who does not pay his debts, but because, if he does not pay his debts, he will lose his credit.'

[21] *Yahoo! Inc.* v. *LICRA and UEJF*, 145 F Supp 2d 1168 (ND Cal. 2001), reversed in *Yahoo! Inc.* v. *LICRA and UEJF*, 379 F 3d 1120 (9th Cir. 2004).

[22] *Yahoo! Inc.* v. *LICRA and UEJF*, 169 F Supp 2d 1181 (ND Cal. 2001).

[23] Eight of the eleven judges found in favour of personal jurisdiction and five of those in favour of ripeness (hereinafter, the minority), but, once the votes of the three judges finding against ripeness (hereinafter, the majority) were added to the votes of the three judges who had found against personal jurisdiction (and by implication against ripeness), there was a six-to-five majority in favour of dismissal of the suit.

[24] The ripeness issue in particular reflects this: a court refuses to exercise jurisdiction when the issue or question to be considered by the court is deemed unripe or unfit for judicial decision because of 'problems of prematurity or abstractness'. *Socialist Labor Party* v. *Gilligan*, 406 US 583, 588 (1972).

enforcement of the French order, but rather in a decision which left the possibility of enforceability open, however remote. In fact, LICRA had not appealed the issue of the enforceability of the French order. It is evident that a clear majority would have found against it – either on the basis that the French order was an act-of-State or on the basis that the private law order, although in principle enforceable in the US, would not be enforced as being contrary to US public policy.[25] But no such decision was made, and, as the court said, '[u]ntil that contention is endorsed by the judgment of an American court, it is only a contention'.[26]

B. 'Voluntary' compliance without the threat of enforcement

There was no real dispute because LICRA had not gone to a US court to ask for the French order to be enforced. If it had done so, neither of the stumbling blocks, personal jurisdiction and ripeness, would have arisen.[27] The most obvious reasons for LICRA's disinterest in actual enforcement are that Yahoo! Inc. had already substantially complied with the French order and that the chances of gaining an enforcement order would have been very slim indeed. In respect of Yahoo's compliance, two questions are of present interest.

First, why did Yahoo! Inc. comply with the French order in the absence of a real threat of enforcement?[28] Yahoo! Inc. itself strongly insisted that changing its website's policy to prohibit the sale of hate speech items was not 'in response to the French court's orders, but rather for independent reasons'.[29] This is consistent with the argument made below, that the principal purpose behind Yahoo! Inc.'s litigation in the US was to establish the illegitimacy of the order, that is, it was an

[25] As the issue of enforceability had not been appealed by LICRA, it was not within the remit of the court to decide it. The majority (Fletcher J, Schroeder CJ, Gould J) left enforceability open as a possibility. Yet, six out of the eleven judges expressly held that the order would not be enforceable in the US: the minority on public-policy grounds, being contrary to the First Amendment, and Ferguson J on the ground that the case was an act-of-State. Tashima J and O'Scannlain J expressed no opinion on the matter.

[26] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1211 (9th Cir. 2006).

[27] By asking the court for the enforcement of the French order, it would have submitted to the court's jurisdiction (see e.g. *Yahoo! Inc.* v. *LICRA and UEJF*, 379 F 3d 1120, 1123 (9th Cir. 2004)) and at the same time the dispute would also have become a real controversy and thus pre-empted the unripeness objection.

[28] Yahoo! Inc. changed its policy in early 2001 before the District Court found the French order unenforceable; nevertheless, even then, the enforceability of the French order would have been very unlikely in view of First Amendment jurisprudence.

[29] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1205 (9th Cir. 2006).

order with which, Yahoo! Inc. asserted, it ought not to comply. So was it just an odd coincidence that Yahoo! Inc. happened to change its policy shortly after the French orders were made? Hardly. Those 'independent reasons' are to be found in the standard considerations of for-profit companies. Although hate speech is legally tolerated in the US,[30] Yahoo! Inc.'s commercial image would not have gained from being seen to condone the sale of Nazi memorabilia by third parties via its website. Its change of policy coincided with the French orders because the French litigation brought Yahoo! Inc.'s old policy into the limelight. So, in effect, legal compliance was compelled indirectly, through channels other than formal legal ones.[31] But equally, Yahoo! Inc. responded to the market only because the market was likely to respond to Yahoo! Inc.'s behaviour after it had been exposed by the litigation. In short, even in the absence of enforceability, factors such as market forces or moral beliefs, or a combination of them, may by themselves or in combination with legal measures compel legal compliance.

C. Enforceability and why it really matters

The second question Yahoo! Inc.'s compliance raises is: if it substantially complied with the order, why did it then seek a court declaration that the order was unenforceable? Why is enforceability in principle or, as the case may be, unenforceability, important? Most obviously, enforceability entails the potential of actual enforcement which is costly either by virtue of the actions necessary to ensure compliance or the sanctions incurred for non-compliance. But, as Yahoo! Inc. had already substantially complied, making enforcement unlikely (despite Yahoo! Inc.'s assertion to the contrary[32]), this ground would hardly have been a factor

[30] *Brandenburg* v. *Ohio*, 395 US 444 (1969).

[31] On the factors that influence behaviour and how they may be manipulated, see Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999); Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501; Albert J. Reiss, 'Selecting Strategies of Social Control over Organisational Life', in K. Hawkins and J. Thomas (eds.), *Enforcing Regulation* (Boston: Kluwer-Nijhoff, 1984), 23; Keith Hawkins, *Environment and Enforcement: Regulation and the Social Definition of Pollution* (Oxford: Clarendon Press, 1984), Ch. 10; Ian Ayres and John Braithwaite, *Responsive Regulation – Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992).

[32] Yahoo! Inc. represented to the court that, even after its change of policy, it was acting in violation of the orders and that it feared that it may be subject to a substantial and increasing fine if it did not take further steps to comply with the French order fully.

justifying years of expensive litigation. More importantly, a decision against enforceability would have set a precedent applicable to much of Yahoo! Inc.'s online activities outside US borders. Yahoo! Inc. would have been assured that its non-compliance with foreign law would not, or would only rarely, entail real repercussions. This, however, assumes that companies like Yahoo! Inc. are comfortable flouting foreign laws – which is clearly not the case. Most high-profile online businesses make a determined effort to comply with the laws of targeted States by, for example, having specially tailored sites which are compliant with local law, managed by local subsidiaries, even when evasion of local law would easily be possible.[33] Such compliance efforts had not saved Yahoo! Inc., but it had tried.[34] The fact is that being perceived as a law-breaker is not good for business. Success in the market, particularly the online market, demands respectability and respectability demands respect for the law.

This explains why Yahoo! Inc. was so keen on a declaration of the French order's unenforceability. The declaration was not designed to allow Yahoo! Inc. to flout foreign laws *per se*, but to flout them under the cover of legality. It wanted to be seen to comply with them *as much as* could *legitimately* be expected – which may be not at all. If French law happened to be repugnant to the US First Amendment (the US being Yahoo! Inc.'s first country of allegiance), legal compliance could not be expected. Yahoo! Inc. hoped US courts would legally sanction its freedom, and perhaps even its moral duty,[35] not to comply with French or other foreign law. As Fletcher J (to the protest of the other judges) noted: 'Yahoo! is necessarily arguing that it has a First Amendment right to violate French criminal law and to facilitate the violation of French criminal law by others.'[36] Yahoo! Inc. wanted its customers in the US, and possibly worldwide, to know that it takes its legal obligations seriously, but only the legitimate ones.

In the transnational setting, a judgment on the enforceability of a foreign law is in effect a judgment on the foreign law's legitimacy in two

LICRA disputed that Yahoo was non-compliant. *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1210 (9th Cir. 2006).

[33] They could do so by avoiding any physical presence, such as offices and assets, in targeted States.

[34] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1202 (9th Cir. 2006).

[35] Not a legal duty as the First Amendment could not forbid Yahoo to impose speech restrictions on its site.

[36] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1221 (9th Cir. 2006), see also 1211: 'the very existence of those [French] orders may be thought to cast a shadow on the legality of Yahoo's current policy'; see *ibid.*, 1244 for the view of the minority.

ways:[37] the legitimacy of its application in the particular circumstances[38] and its substantive legitimacy.[39] Was it legitimate for France to apply its law to Yahoo! Inc. and its general website, i.e. was it within its regulatory competence? Furthermore, was the French prohibition of the sale of Nazi memorabilia a good law, i.e. was it reconcilable with US public policy? If either of the answers is no, the legal obligation under foreign law is illegitimate and thus not enforceable. The general upshot is that the enforceability of a law is important not just because it lets legal subjects know that compliance could be compelled, but also because it reinforces or perhaps even establishes the law's legitimacy. And legitimacy itself may be sufficient to induce compliance simply based on a moral belief that legitimate laws ought be complied with, or because of the need to be seen to comply with legitimate laws. Yahoo! Inc.'s action was based on both: Yahoo! Inc. wanted to be seen to comply with its legitimate legal obligations because most of its customers believe that one ought to comply with one's legitimate legal obligations. The practical implication is that, if States were generous with finding each other's laws enforceable, it would go quite some way towards inducing respect for foreign laws, even without actual enforcement.

However, a law's legitimacy has its limitations as a factor compelling compliance. Not all individuals hold a belief, or rather always act upon their belief, that legitimate legal obligations demand respect.[40] Such a belief may, for example, be trumped by the prospect of the benefits to be gained from non-compliance, including saving the cost of compliance. Commercial companies in particular tend to take an amoral stance on their legal duties. The cost of compliance is simply put into a general

[37] Note it also passes a judgment on the perceived respectability or impartiality of the foreign judicial system, see e.g. §482(1)(a) of the US Restatement (Third) of Foreign Relations Law (1986); under English law, this would appear to fall under the fraud defence: J. G. Collier, *Conflict of Laws (*3rd edn, Cambridge: Cambridge University Press, 2001), 119.

[38] For the position under English law, see e.g. *Adams* v. *Cape Industries plc* [1990] Ch 433 (CA) (foreign court lacked personal jurisdiction over defendant); see also §482(1)(b) and (2)(a) of the US Restatement (Third) of Foreign Relations Law (1986) and §104 of the US Restatement (Second) of Conflict of Laws (1971).

[39] This is provided for by the public policy exception, see below n. 60, for the position under English law, see e.g. *Kuwait Airways Corp.* v. *Iraqi Airways Co*. [2002] UKHL 19, para. 17; see also §482(2)(d) of the US Restatement (Third) of Foreign Relations Law (1986) and §117 of the US Restatement (Second) of Conflict of Laws (1971).

[40] This is perhaps where Hart's argument – that sanctions are not needed, as 'the normal motive for obedience, but as a *guarantee* that those who would voluntarily obey shall not be sacrificed to those who would not' – becomes relevant. Hart, above n. 15, 198 (emphasis in the original).

cost–benefit analysis: if the risk of a sanction being imposed is small, even where the sanction is relatively severe, it may well be more profitable not to comply with the legal obligations and take the risk. However, the moral duty of legal compliance can be imposed on amoral commercial actors via the market, as occurred in the Yahoo saga.[41] But the market can only respond if there is sufficient publicity of an actor's legal non-compliance. If the risk of such exposure is remote, there will be far less pressure on commercial actors to comply.

In short, the legitimacy of a law or court order by itself is not always a good enough assurance of legal compliance. Yet this cannot detract from the fact that it often is, and that a judgment in favour of enforceability of a foreign law lends those laws the all-important air of legitimacy. The question is how willing are courts to give their approval to foreign court orders?

3. Upholding local law despite foreign violations

Cooperative willingness by States in respect of their law enforcement depends largely on the private or public nature of the law, dispute or judgment in question. This categorisation, albeit of foundational importance, is often far from clear-cut, as shown further below. For the moment, the question is simply: how far does cooperation go, especially where there is significant divergence in legal norms between States?[42]

A. Cooperation in private law

The litigation by Yahoo! Inc. against LICRA was premised on the assumption that *prima facie* the French order could be enforced in the US. This is based on the general willingness by States to cooperate with each other in respect of each other's private law.[43] This cooperation occurs not just at

[41] Also, smaller, lesser-known businesses would attract much less publicity.

[42] See Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cybercrime?' (2002) 10 *International Journal of Law and Information Technology* 139, where the authors distinguish between crimes against the person, against property, against the State and against morality, noting that there is a significant legal consensus in respect of the first two groups, but not in respect of the latter two.

For insightful discussions on the dynamics of cooperation between 'self-seeking egoists', see Robert Axelrod, *The Evolution of Co-operation* (first published 1984, London: Penguin Books, 1990); Robert Axelrod, *The Complexity of Cooperation* (Princeton: Princeton University Press, 1997).

[43] The ambit of this cooperation has been subject to extensive debate: see e.g. Gerrit Betlem, 'Transboundary Enforcement: Free Movement of Injunction', in Sven

the margins of law enforcement, but in two substantive ways: the willingness to apply foreign substantive law to disputes heard in local courts and the willingness to enforce judgments handed down in foreign courts. The existence of such cooperation in law enforcement means that *prima facie* transnational activity need not be a threat to the effectiveness of national law; its effectiveness can be assured with the help of other States.

This willingness to cooperate is not based on any obligation under customary international law to cooperate.[44] Indeed, customary international law does not concern itself with State competence over private matters.[45] Similarly, high-minded notions, such as comity or respect for sovereign States,[46] also hold less sway as a basis to explain cooperation[47] than more practical considerations, such as fairness or convenience to the parties. Whatever the reasons may be, State cooperation at the enforcement stage is highly beneficial because it allows States to uphold their local laws even when they would otherwise lack power over foreign wrongdoers.[48]

Deimann and Bernard Dyssli (eds.), *Environmental Rights – Law, Litigation and Access to Justice* (London: Cameron May, 1995), 184; Antonio I. Pribetic, '"Strangers in a Strange Land" – Transnational Litigation, Foreign Judgment Recognition, and Enforcement in Ontario' (2004) 13 *Journal of Transnational Law and Policy* 347.

[44] But much of this cooperation is enshrined in bilateral treaties, e.g. Agreement between the Government of Australia and the Government of the United Kingdom of Great Britain and Northern Ireland providing for the Reciprocal Recognition and Enforcement of Judgments in Civil and Commercial Matters (1990).

[45] Akehurst, above n. 2, 222; Sir Robert Jennings and Sir Arthur Watts (eds.), *Oppenheim's International Law* (9th edn, London: Longman, 1992), Vol. 1, 6f, 488ff; Gerfried Mutz, 'Private International Law', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 330, 340. There is some significant dissent: Mann (1973), above n. 2, 131, 134; Ian Brownlie, *Principles of Public International Law* (4th edn, Oxford: Clarendon Press, 1990), 299. There is, however, a growing body of public international law in the form of treaties covering private international law matters: see e.g. Hague Conference on Private International Law, www.hcch.net.

[46] Akehurst, above n. 2, 217ff, noting the origins of these notions in the writings of Ulric Huber, Joseph Story and Savigny.

[47] R. H. Graveson, *Comparative Conflict of Laws* (Oxford: North-Holland Publishing Company, 1977), Vol. 1, 17, 21, quoting Dicey: 'the application of foreign law is not a matter of caprice or option, it does not arise from the desire of the sovereign of England, or any other sovereigns, to show courtesy to other states. It flows from the impossibility of otherwise determining whole classes of cases without gross inconvenience and injustice to litigants, whether natives or foreigners.'

[48] William S. Dodge, 'Antitrust and the Draft Hague Judgments Convention' (2001) 33 *Law and Policy in International Business* 363, 364, where the author – noting that the US due to its size tends to be better positioned to give its antitrust legislation an outward

Cooperation and regulatory restraint

Another more indirect, but equally important, benefit of cooperation is that it provides an incentive for regulatory restraint; cooperation has a moderating effect on the regulatory claims States assert in the first place. This is partly explicable by virtue of the fact that, with a willingness to cooperate looming in the background, there is less urgency to grab regulatory control whenever enforcement power is present, no matter how tenuous the connection.[49] Knowing that a foreign court would adjudicate the dispute, possibly applying the same substantive law, makes it easier to refuse jurisdiction when the connection with the State is weak. Cooperation gives the freedom not to assert jurisdiction in favour of a State with the stronger connection. Conversely, in, for example, *Dow Jones & Co. Inc.* v. *Gutnick*,[50] the assertion of adjudicative jurisdiction by an Australian court was easily justifiable as it was clear that the US – as the State with the stronger overall connection to the facts – would not be willing to recognise Gutnick's defamation claim under either US or Australian law.[51] Justice would not be done. Furthermore, the High Court of Australia felt that it could rely on a nexus so weak as to give rise to global liability, because such global liability was only theoretical; it was theoretical only because the frequent refusal to cooperate at the enforcement stage would deter many would-be litigants.[52]

Secondly, cooperation also encourages more moderate regulatory assertions by States and their courts because generally their judgments are only enforceable abroad if they exercised regulatory restraint. This is formally incorporated into the review of the foreign judgment: it is only

reach – still argues for reciprocal enforcement of antitrust judgments, as that would benefit smaller States. Note, the practical difficulties and costs associated with bringing an action abroad or seeking the enforcement of a judgment in a foreign court make transnational litigation unrealistic in the consumer context.

[49] Mann (1973), above n. 2, 127f: because a State cannot hope for cooperation by other States in enforcing its laws in respect of activity that impacts on its territory, it attempts (at least on those occasions when it has enforcement power) to compensate for this by 'resort[ing] to its own legal system and, in particular, its own courts for the purposes of making the conduct of foreigners in foreign countries conform to its own command'.

[50] [2002] HCA 56.

[51] In the Australian action, Gutnick, for tactical reasons, had limited his claim to the damage he had suffered in Australia, although on the facts it appeared that the damage to his reputation may well have been greater in the US, where he enjoyed a reputation and where most of the readers of the site were located.

[52] *Dow Jones & Co. Inc.* v. *Gutnick*, [2002] HCA 56, para. 53, 165; see also Chapter 4, nn. 80 and 81 and the accompanying text.

enforced if the foreign court did not exceed its adjudicative or legislative jurisdiction according to the enforcing State.[53] By refusing cooperation when there was an excessive assertion of competence, States mutually police the moderateness of regulatory assertions. Yahoo! Inc. disputed the Paris court's competence on the basis that the act in question was committed in the US, its servers were there and the activities were directed at the US,[54] and those objections it restated before the US court.[55] Without expressly addressing the issue of France's competence in this case, the District Court in California noted that a 'basic function of a sovereign state is to determine by law what forms of speech and conduct are acceptable within its borders . . . France clearly has the right to enact and enforce laws as those relied upon by the French court here'.[56] This suggests that France's exercise of regulatory competence was considered reasonable by the US court. Yet, in fact, the US court's generosity was perhaps no more than introductory rhetoric to soften the blow of the refusal of cooperation on another ground, i.e. the public policy ground. Generally, refusal to enforce a law on the basis of excessive jurisdiction is a ground which does not look to the substance of the foreign law and its relative compatibility with the law of the enforcing State. This means that substantive legal differences do not present a hurdle to enforcement at this stage; tolerance for substantive differences is still legally provided for.

In short, cooperation in the enforcement of each other's laws is beneficial, and not just in terms of inducing compliance with national law in the transnational context. It creates real incentives for States to exercise regulatory restraint, which in turn reduces the number of

[53] See above n. 38.

[54] *LICRA* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000); *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000).

[55] Complaint for Declaratory Relief, *Yahoo! Inc.* v. *LICRA*, No. C 00-21275 (PVT) (ND Cal., 21 December 2000), para. 19, 42(c) and (f); see also ABA, above n. 4, 92, noting that recognition is denied if there was a 'violation of procedural due process, lack of personal jurisdiction by the rendering court, or, in rare instances, violations of public policy in the recognition state' (footnotes omitted).

[56] *Yahoo! Inc.* v. *LICRA and UEJF*, 169 F Supp 2d 1181, 1186 (ND Cal. 2001), see also 1191f: 'Although France has the sovereign right to regulate what speech is permissible in France, this Court may not enforce a foreign order that violates the protection of the United States Constitution by chilling protected speech that occurs simultaneously without our borders.'

concurrent claims and contributes to a more orderly transnational legal world.

Two interpretations of the 'public policy' exception

States refuse cooperation in the private law context where enforcement of the foreign judgment would be contrary to their public policy. This exclusionary rule is widely adopted, and has been expressed under English law as follows:

> English courts will not enforce or recognise a right, power, capacity, disability or legal relationship arising under the law of a foreign country, if the enforcement or recognition of such right, power, capacity, disability or legal relationship would be inconsistent with the fundamental public policy of English law.[57]

This public-policy exception marks the outer boundaries of States' tolerance for each other's legal differences. But when is a foreign law so intolerable that it cannot be enforced? Does the public-policy exception import a requirement of relative uniformity or at least compatibility of legal standards? Clearly, the greater the readiness to rely on the exception, the greater the problems States face in upholding their peculiar private law standards – a matter of not inconsiderable concern in the online environment.

No comprehensive exploration of how different States interpret the exception can be attempted here.[58] Instead, *Yahoo* is used to show possible alternative interpretations and their ramifications. The exception was central to two of the three separate decisions in *Yahoo* even if only indirectly as part of the ripeness issue. These two decisions reflect two fundamentally different understandings of the exception, and what level of tolerance ought to be accorded to foreign law. In *Yahoo*, all the judges agreed that the French order laid down a speech standard stricter than US speech standards. Varying legal standards are often present in enforcement scenarios, which in itself is not a problem: 'foreign laws need not be identical to . . . the laws of the United States; they merely

[57] Lawrence Collins (ed.), *Dicey and Morris on Conflict of Laws* (13th edn, London: Sweet & Maxwell, 2000); Vol. 1, 81; see also §482(2)(d) of the US Restatement (Third) of Foreign Relations Law (1986) and §117 of the US Restatement (Second) of Conflict of Laws (1971); discussed e.g. in Jeremy Maltby, 'Juggling Comity and Self-Government: The Enforcement of Foreign Libel Judgments in US Courts' (1994) 94 *Columbia Law Review* 1978, 2008ff.

[58] There are as many interpretations as there are States, and indeed more.

must not be repugnant to our laws and policies.'[59] So differences are acceptable as long as they are not intolerable or, more formally, 'repugnant to fundamental principles of what is decent and just'.[60] While such principles of basic decency and justice could conceivably be derived from internationally recognised norms such as human rights norms, as they reflect what the international community treats as the 'just and decent' minimum. In fact, they are not, or at least not just.[61] States supply their own views of decency, and these views may vary significantly. But, again, this would often not stand in the way of cooperation if States, except in very exceptional circumstances, respected other States' views on decency and justice as far as the others' citizens were concerned, even if not sharing them in respect of their own.

And this is where the judges in *Yahoo* disagreed. According to the three judges of the ultimate majority (hereinafter, the majority), it could not be decided whether the French order was repugnant to US public policy,[62] as it was not clear what, if anything, the order would require Yahoo! Inc. to do beyond what it had done already of its own free volition. More specifically, whether the First Amendment was offended by the French order would at least partly depend on whether any additional compliance action by Yahoo! Inc. would also have an impact on access to its site from US territory.[63] In that event, the public-policy exception would almost certainly demand non-enforcement of the French order. On the other hand, if the French court's demand – that

[59] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1215 (9th Cir. 2006), citing *In re Schimmelpenninck*, 183 F 3d 347, 365 (5th Cir. 1999). The same is the position in England, see e.g. *Phrantzes* v. *Argenti* [1960] 2 QB 19 (CA), where the court held that the action would not fail merely because the cause of action was unknown to English law, or *Kuwait Airways Corp.* v. *Iraqi Airways Co.* [2002] UKHL 19, para. 15, on the acceptability of legal differences.

[60] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1215 (9th Cir. 2006), citing *Turner Entertainment Co.* v. *Degeto Film GmbH*, 25 F 3d 1512, 1519 (11th Cir. 1994). In England, the House of Lords in *Kuwait Airways Corp.* v. *Iraqi Airways Co.* [2002] UKHL 19, para. 17, citing with approval *Loucks* v. *Standard Oil Co. of New York*, 120 NE 198, 202 (1918): a foreign decree would be excluded if it 'would violate some fundamental principle of justice, some prevalent conception of good morals, some deep-rooted tradition of the common weal'.

[61] *Kuwait Airways Corp.* v. *Iraqi Airways Co.* [2002] UKHL 19, para. 18.

[62] Strictly speaking, in *Yahoo* the question was whether the French order was repugnant to *California's* public policy. *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1212, 1239 (9th Cir. 2006), but the difference between the Californian Constitution and the US federal Constitution is marginal and of no further relevance here.

[63] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1216f (9th Cir. 2006).

access to Nazi memorabilia be denied only to users from France – could be achieved without affecting US users' access, then, according to the majority, the legal issue was entirely different. If the French order would concern only activities on French territory, would US public policy still be offended by the stricter French laws? Should the First Amendment apply to extraterritorial events or should France's view on speech be respected? The majority held that the issue of the extraterritorial reach of the First Amendment was still unresolved,[64] and would not be decided in this case, given that it was unclear on the facts what legal question in fact required determination.

The five judges of the final dissent (hereinafter, the minority) showed much less hesitation in finding, first, that the enforceability issue was ripe for adjudication and, secondly, that the French order was repugnant to US public policy and thus unenforceable. The minority held that the French order offended US public policy, not because the First Amendment applies to Yahoo! Inc.'s activities outside the US,[65] but rather because the order required Yahoo! Inc. to take certain actions *within* the US (and these were insufficiently defined in the overbroad and vague French order[66]): 'Yahoo! has . . . First Amendment protection from being sanctioned when it could not guess or it guessed wrong as to what it was supposed to censor on its domestic servers – even if limited to France-based users.'[67]

The reasoning of the minority is misleading. Its decision necessarily means that the First Amendment would be applied to events *outside* the US, thereby overriding other States' stricter speech standards in their own territories. This is because whenever the enforcement of a foreign judgment is sought, the whole point is to make the defendant do something in the enforcing State. If the locality of that act is used to assert that the foreign order must be compatible with local law, then the foreign judgment will always have to comply with local law – even if the internal act only takes effect abroad. The minority seems to recognise this and notes that legal differences vary in their profundity. There are 'foreign orders that are somewhat inconsistent with US law . . . [and] those that violate US law'.[68] And a 'violation' (which entails non-enforcement) is

[64] Citing *Desai* v. *Hersh*, 719 F Supp 670 (ND Ill. 1989); *Laker Airways Ltd* v. *Pan American Airways Inc*., 604 F Supp 280 (DCC 1984); *Bullfrog Films Inc.* v. *Wick*, 646 F Supp 492 (CD Cal. 1986).

[65] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1234f (9th Cir. 2006).

[66] *Ibid*., 1235. [67] *Ibid*., 1235f. [68] *Ibid*., 1240.

involved whenever the judgment would be unconstitutional if it had been handed down by a US court. In clear text, foreign judgments have to be consistent with the US constitution to be enforceable, no matter whether they take effect inside or outside US borders.[69]

The minority approach is understandable in so far as a State's constitutional Bill of Rights reflects its most treasured values and what it considers 'just and decent'. If a foreign judgment would have the effect of undermining those values, cooperation could legitimately be denied. But the French court took pains to ensure that its order would not spill over to other shores and that it would be restricted in its effect to France. So, even if a US court enforced the French orders, the more permissive legal standard would be entirely intact in the US. In these circumstances, one cannot but wonder why more tolerance and respect are not shown for another State's fundamental values. This is particularly so as cooperation would be beneficial for all States. Furthermore, while French free-speech standards are stricter than those in the US, the difference would not appear to be so great as to make the French standard abhorrent and morally impermissible. Both States share a profound commitment to free speech and would condemn neo-Nazi, anti-Semitic and racist sentiments.[70] And, although they differ in their view of how democracy can best be achieved,[71] both are committed to the democratic ideal. So helping the other State to enforce its speech laws within its own territory would hardly involve any insurmountable moral dilemma. And yet, of the eleven judges in *Yahoo*, only three expressly left enforceability open as a possibility.[72]

The public-policy exception provides an indispensable escape route for States willing in principle to cooperate with each other in the enforcement

[69] *Ibid*., 1240.

[70] *Ibid*., 1240, where even the minority acknowledged: 'People in the United States and France should abhor anti-Semitism and the horrors perpetrated by the Nazi Party. Nonetheless, our constitutional law differs from French jurisprudence in our approach to hate speech. Our law reflects deeply held political beliefs about freedom of expression in this country . . . [T]he remedy to be applied to expose falsehood and fallacies is more speech, not enforced silence.' See also Council of Europe, Recommendation No. R(97)20E of the Committee of Ministers to Member States on 'Hate Speech' (adopted by the Committee of Ministers on 30 October 1997); Council of Europe's Additional Protocol to the Cybercrime Convention, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (adopted by the Committee of Ministers on 7 November 2002, came into force on 1 March 2006). France, but not the US, is a party to the Protocol.

[71] *Yahoo! Inc*. v. *LICRA and UEJF*, 433 F 3d 1199, 1240 (9th Cir. 2006).

[72] See above n. 25.

of their private laws. But, unless used sparingly,[73] it undermines the cooperation regime.[74] As the majority suggested, there are fundamentally two types of situations in relation to which the public-policy exception should operate differently: first, where the judgment would have an effect within the enforcing State and, secondly, when it would not. In the former case, it would seem entirely legitimate to assess the judgment's compatibility with local legal standards, in particular constitutional norms, and if there is a conflict refuse enforcement. If the French order had an effect on free-speech standards in the US, cooperation is legitimately dependent on the compatibility of the foreign order with US free-speech law. On the other hand, where the judgment is to take effect only outside the borders of the enforcing State, there should be a presumption for enforcement to be rebutted only when the foreign law is so abhorrent as to be irreconcilable with 'justice or decency' or 'good morals'. And, to equate 'justice and decency' here with one's own constitutional standard, as the minority did, seems parochial indeed – foreclosing cooperation when not much tolerance is asked for, and much is to be gained from it. The question *Yahoo* crystallises is: why is there such resistance to cooperation? That question becomes even more prominent in the public law context.

B. No cooperation in public law

The 'public law' taboo[75]

The French Yahoo case is a boundary case. It hovers somewhere between the private-law and the public-law realms. Three of the eleven judges held that the significant financial penalty attached to the French order would not

[73] States differ in their readiness to invoke this rule, but US courts have shown little hesitation in using it in the free speech context: Kyo Ho Yum, 'The Interaction Between American and Foreign Libel Law: US Courts Refuse to Enforce English Libel Judgments' (2000) 49 *International and Comparative Law Quarterly* 132.

[74] Collins, above n. 57, 81: 'In the conflict of laws it is even more necessary that the doctrine should be kept within proper limits, otherwise the whole basis of the system is liable to be frustrated'; William E. Holder, 'Public Policy and National Preferences: The Exclusion of Foreign Law in English Private International Law' (1969) 17 *International and Comparative Law Quarterly* 926, 928, arguing that 'the operation of public policy tends to be a negation of the co-operation of national institutions which lies at the base of effective enforcement of foreign prescriptions.' In contrast, the exclusionary rules on foreign public law merely define the outer boundaries of private international law.

[75] Term coined by Andreas F. Lowenfeld, 'Public Law in the International Arena: Conflict of Laws, International Law and Some Suggestions for their Interaction' (1979) 163 *Recueil des Cours* 311, 322ff.

be enforceable if it came to it on the basis of its being an unenforceable public-law fine.[76] In addition, Ferguson J held the order to be non-justiciable on the basis of its being an act-of-state.[77] Both grounds fall broadly within the universal non-cooperation stance in respect of foreign public or criminal laws, judgments or acts.[78] Courts refuse to allow for their own public law to be replaced by a foreign public law[79] and are also unwilling to enforce a foreign public-law judgement:[80] 'courts have no jurisdiction to entertain an action . . . for the enforcement, either directly or indirectly, of a penal, revenue or other public law of a foreign State.'[81] This rule has a long and steady history and withstood many challenges quite unharmed.

[76] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1218 (9th Cir. 2006). Note the majority appears to characterise the penalty to induce compliance with the injunction as public, while the injunction itself is characterised as private, which seems somewhat illogical. See the discussion below.

[77] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1225ff (9th Cir. 2006).

[78] Having said that, the act-of-state doctrine is traditionally an offshoot of State immunity, and immunises agents and officials from being sued or prosecuted in one State for acts carried out on behalf of another State. So the act-of-State doctrine, like State immunity, ought not to be applicable where the State or its officials are the plaintiffs, that is, it ought not to prevent them from benefiting from actions. Akehurst, above n. 2, 240ff, esp. 245.

[79] This is so even if it runs counter to the normal choice-of-law rules or the express election by the parties. For a rare case where a party was allowed to contract out of a State's public law, see *R* v. *Harden* [1963] 1 QB 8. See also Philip J. McConnaughay, 'Reviving the "Public Law Taboo" in the International Conflicts of Law' (1999) 35 *Stanford Journal of International Law* 255, 280.

[80] At times States have gone even further and expressly prohibited defendants from complying with the foreign order based on foreign public law: *British Nylon Spinners* v. *Imperial Chemical Industries* [1953] Ch 19. Australian Law Reform Commission, *Choice of Law*, Report No. 58 (1992), para. 8.15: 'The English courts have on occasion refused to enforce contracts the object of which is to break the laws of a friendly foreign country . . . It did not matter that the foreign law was undoubtedly a penal law.' But note, there is limited recognition of foreign public law where it supplies a datum for the application of domestic private law or is determinative of a preliminary matter: see e.g. *Williams & Humbert* v. *W & H Trade Marks* [1986] 2 WLR 24, where the House of Lords held that the principle that a country could not collect its taxes outside its territory could not stop the English court from recognising, without considering the merits, the compulsory acquisition laws of a foreign State and acknowledge the changes of title to property which came under the control of that State. Hans W. Baade, 'The Operation of Foreign Public Law' (1995) 30 *Texas International Law Journal* 429, 447ff. See Comment e to §483 of the US Restatement (Third) of Foreign Relations Law (1986): 'Judgments not entitled to enforcement under this section may nevertheless be recognized for certain purposes. For instance, a foreign conviction of a crime may be recognized for purposes of denying the convicted person a visa or naturalization.'

[81] Collins, above n. 57, 89. In *US* v. *Inkley* [1989] QB 255, 264, the court noted: 'the enforcement of public law . . . [is] the general umbrella under which both penal and

The effect of this rule is exactly the same as that of the public-policy exception: the enforceability of the foreign law or judgment is denied. However, basing unenforceability on the public-law status of the foreign law is said to be the 'safer' option: there is no need to evaluate the foreign law substantively and thereby create the potential for embarrassment and straining of relations between States.[82] Saying a foreign law or judgment is unenforceable simply because it is public in nature involves ostensibly only a 'neutral' assessment of its character.[83]

But whatever advantages this public-law taboo has in tactical terms, the rule as such is deeply worrying. It creates a vast area of law and regulation in the online and offline context in respect of which States are left entirely to their own devices. Cases like *Yahoo* are the few hard cases which make it into the courtrooms, but for each of these there are innumerable clear-cut public-law cases where foreign cooperation would very clearly be ruled out. Again, this concern is particularly acute in the context of non-harmonised legal standards. Where States share similar views as, for example, in respect of protecting personal property (e.g. online hacking) or the physical integrity of people (e.g. online child pornography), each State, by enforcing its laws over local wrongdoers, indirectly helps to protect the legal standards of other States. But, in respect of those laws which reflect very different political, cultural or religious standards, and more broadly the different moral fabrics of societies,[84] the combination of the Internet and the public-law taboo is problematic. Western democratic States are, in particular, vulnerable with regard to much foreign content infiltrating their territories and

revenue suits are embraced'; see also the discussion in *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 41f.

[82] *Moore* v. *Mitchell*, 30 F 2d 600, 604 (1929).

[83] See e.g. Thomas B. Stoel, 'The Enforcement of Foreign Non-Criminal Penal and Revenue Judgments in England and the United States' (1967) 16 *International and Comparative Law Quarterly* 663, 670; McConnaughay, above n. 79, 267: 'Judicial analysis concerning the applicability of public law, in contrast, traditionally ends where conflicts analysis begins: If the court determines that the forum's public law applies . . . it does not proceed further to consider the parties' expectations or some other nation's possible superior interest in the transaction or issue'; Mann (1971), above n. 2, 183; Holder, above n. 74, 926, where the author notes that, while the rule offers great flexibility, it is an 'unruly horse' that cannot provide the predictability and certainty concrete rules do.

[84] Goodman and Brenner, above n. 42; Smith, above n. 4, 525; Bremer, above n. 4, 206ff.

undermining local policies.[85] The unilateral measures they can adopt within their own borders are, as shown below, imperfect at best. This raises yet again the all-important question: why do States so strongly resist cooperation in the enforcement of each other's laws when it would be so mutually beneficial?

Lack of power or lack of will?

Can States not cooperate, or do they not want to? Authorities on this seemingly simple question are divided. One viewpoint is exemplified by the majority in *Yahoo*, which relied on §483 of the US Restatement (Third) of Foreign Relations Law (1986). This states that US courts 'are *not required* to recognize or to enforce judgments for the collection of taxes, fines, or penalties rendered by the courts of other states'.[86] This clearly implies that they could, but need not, enforce such judgments. The comment on the section goes on to state that '[n]o rule of United States law or of international law would be violated if a court in the United States enforced a judgment of a foreign court'.[87]

In contrast, Ferguson J argued that the lower court[88] ought to have abstained from deciding the claim as '[e]very foreign state is *bound to respect* the independence of every other sovereign state, and the court of one country will not sit in judgment on the acts of government of another'.[89] According to Ferguson J, the court simply had no power to pass judgment on the foreign public act. And, although he relied on the act-of-State doctrine, the same apparent respect for international law and foreign States' rights is often advanced as a reason for denying the enforcement of foreign public-law judgments. In *Huntington* v. *Attrill*,

[85] See the discussion below on unilateral enforcement strategies.

[86] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1219 (9th Cir. 2006) (emphasis added, parenthesis in the original); at *ibid.*, 1218, the majority asserted that the non-enforcement rule applies unless there is a treaty to the contrary effect. To the author's knowledge, no such treaty providing for the mutual enforcement of foreign penalties exists (recent EU developments apart: see below n. 221).

[87] Comment a. to §483 of the US Restatement (Third) of Foreign Relations Law (1986).

[88] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1225f (9th Cir. 2006). Ferguson J asserted that the case was simply beyond the authority of the 'District Judge . . . [who] should have deferred to the Executive and Congress to assess the foreign consequences of France's broad policy against antiSemitic hate speech'. This implies that the executive might have expressed a willingness to cooperate in the enforcement of the French law. Again, to the author's knowledge, such action would have been entirely unprecedented.

[89] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1225f (9th Cir. 2006) (emphasis added), relying on *Underhill* v. *Hernandez*, 168 US 250 (1897); *Banco Nacional de Cuba* v. *Sabbatino*, 376 US 398 (1964); *Liu* v. *Republic of China*, 892 F 2d 1419 (9th Cir. 1989).

the US Supreme Court noted that, when 'a statute . . . is a penal law in the international sense . . . it *cannot* be enforced in the courts of another state'.[90] In *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd*, the Australian High Court stated: '[T]he right or interest asserted in the proceedings is to be classified as a governmental interest. As such, the action falls within *the rule of international law* which renders the claim unenforceable.'[91] So are State indeed prohibited from enforcing foreign public laws?

First of all, along the same lines as the above argument that cooperation affects regulatory claims made in the first place, the non-cooperation in the enforcement of public law has been understood as a mirror image of extraterritorial regulatory claims:[92]

> [I]n the last few decades, the subject [i.e. the extraterritorial status of public law] . . . has stood under the shadow of what is loosely called extraterritorial jurisdiction: the outward reach of the public law of specific countries, and limitations imposed by international law, 'comity', or self-restraint on such assertions of jurisdiction . . . [T]he mirror image of this phenomenon . . . is the treatment of such assertions of extraterritorial jurisdiction by the 'target' state.[93]

The connection was also acknowledged in *Bank voor Handel en Sheepvaart NV* v. *Slatford*: 'English courts will not enforce . . . [foreign public law] since they will treat it as having no extra-territorial effect.'[94] One commentator has gone further and expressly asserted that the non-enforcement of public law is in fact necessary to limit excessive

[90] *Huntington* v. *Attrill*, 146 US 657 (1892) 664 (emphasis added); *AG of New Zealand* v. *Ortiz* [1984] AC 1, 24 (Lord Denning): '"public laws" . . . will not be enforced by the courts of the country to which it is exported, or any other country, because it is an act done in the exercise of sovereign authority which will not be enforced outside its own territory.'

[91] *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 46f (emphasis added).

[92] Both issues are rarely raised in respect of the same case, but exceptionally this has occurred with US antitrust cases. In respect of these cases, the US was accused of exercising excessive jurisdiction under international law over foreign companies in respect of their foreign activities and the courts of other States refused to enforce US judgments against these companies. As many of the actions were brought by private individuals, they sought to enforce them abroad on the basis that they were merely private cases. Generally, States tend not to seek enforcement of their public laws in foreign States and even less so when they know that the foreign State views such exercise of jurisdiction as excessive under international law.

[93] Baade, above n. 80, 431.

[94] *Bank voor Handel en Sheepvaart NV* v. *Slatford* [1953] 1 QB 248, 257.

jurisdictional claims: 'framed in terms of lack of jurisdiction . . . [in fact] it is the foreign State which has no international jurisdiction to enforce its law abroad, and the English court will not exercise its own jurisdiction in aid of an excess of jurisdiction by the foreign State.'[95] This is incorrect, first, because often the initial assertion of adjudicative/legislative jurisdiction falls squarely within the competence rules under international law and is thus not excessive.[96] Furthermore, in respect of enforcing foreign public law, unlike private law, there is never any inquiry whether the other State asserted competence legitimately or not. Secondly, when the foreign State simply and humbly asks for another State's cooperation, the former State cannot possibly violate the non-interference rule or exceed enforcement jurisdiction. Thirdly, were the latter State to consent to that request, any illegitimacy of jurisdiction would be vitiated through the latter State's consent.[97] In short, to argue that non-cooperation is there to curb excessive regulatory claims is simply incorrect; and indeed, as was shown above, a principled willingness to cooperate (unlike the refusal to do so) encourages more moderate regulation.

[95] Collins, above n. 57, 90, approved in *Re State of Norway's Application (Nos. 1 and 2)* [1990] 1 AC 723, 808; see also Mann (1990), above n. 2, 359ff: 'The State which outside the confines of its own sovereignty pursues penal, tax or other public claims invokes its sovereign rights within the territory of the forum. Even the institution of legal proceedings implies the assertion that the plaintiff State is *entitled* to prosecute its public rights in the forum' (emphasis in the original). For other rationales, see Stoel, above n. 83, 668, mentioning a number of reasons, including practical considerations. See also *Lipohar* v. *R* (1999) 168 ALR 8, para. 107 (citing with approval Brilmayer, *An Introduction to Jurisdiction in the American Legal System* (1986), 321): 'In criminal cases, the State is both a party – granted standing to prosecute by statute – and the adjudicative forum – given jurisdiction to decide criminal cases brought by the State against alleged criminals. Because one State cannot validly involve the other's interest as a party on redressing an injury, States do not enforce one another's criminal laws.' Some have additionally argued that enforcement would exceed the judicial function, e.g. Mann (1984), above n. 2, 42: 'No judge is able or entitled to allow such a claim to proceed and thus to permit an excess of international jurisdiction. Such permission can only be given by the sovereign authority itself and almost everywhere presupposes a treaty and legislation. A judge who would take it upon himself to forego his sovereign's right of jurisdiction would prejudice him greatly: he would be deprived of the opportunity to secure reciprocity of treatment.' But see above n. 78.

[96] Above n. 56.

[97] Werner Meng, 'Recognition of Foreign Legislative and Administrative Acts', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 348, 349: 'If a State . . . exercises [excessive extraterritorial] jurisdiction . . . another State is nevertheless free to recognize this sovereign act if no third State's rights are violated.'

Curiously, the very judges who treat other States' rights and international law with so much deference when it comes to the non-enforcement of foreign judgments are the same judges who treat international law with such a cavalier attitude when it comes to their own regulatory competence over foreign matters. As Chapters 3 and 4 show, not only do they constantly push the boundaries of their own State's competence, they also routinely fail to acknowledge that international law is in fact determinative of those powers,[98] and at most refer to the demands of 'international comity'[99] which is not being used as a synonym for international law.[100]

Although it is easier to assert 'I am not allowed to help you' rather than 'I do not want to help you', the better view – which fits more comfortably within international law – is that international law is not prohibitive but permissive in respect of enforcement of a foreign public law. It does not require a State to enforce foreign public law, but does not prohibit it either. This view is consistent with the stance taken by the majority in *Yahoo*. Equally, it was also expressed in a German judgment of 22 March 1983:

> According to public international law a State is in principle under no duty within the limits of its sovereignty to tolerate the performance or execution of acts of sovereignty by another State ... or by way of judicial assistance to render facilities; on the other hand public international law does not prohibit such tolerance or co-operation; it makes them available to States. Extreme diffidence is being displayed by States particularly where the execution within their own sphere of sovereignty of foreign criminal judgments or the collection of foreign revenue claims are concerned.[101]

[98] There can be no doubt that '[t]he existence of the State's right to exercise jurisdiction is exclusively determined by *public international law*' Mann (1973), above n. 2, 4 (emphasis in the original).

[99] See, for example, *Yahoo! Inc.* v. *LICRA*, 169 F Supp 2d 1181, 1192 (ND Cal. 2001), citing *Hilton* v. *Guyot*, 159 US 113, 163f (1895), approved *obiter* in Australia in *Lipohar* v. *R* (1999) 168 ALR 8, 34.

[100] Akehurst, above n. 2, 216; see also Griffin B. Bell, 'International Comity and the Extra-territorial Application of Anti-Trust Laws' (1977) 51 *Australian Law Journal* 801, 803: 'comity is more than a legal principle. It is the expression of a civilised human being and a humane Government – a policy of courtesy, of restraint, of civility, and of concern and sympathy for those with which we deal.'

[101] Discussed and rejected in Mann (1984), above n. 2, 37; see also Karl Doehring, 'State', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 423, 425, where the author asserts that '[e]very government is free to recognize acts of State of other governments producing effects beyond the boundaries of the acting

Finally, in England, this view was also implicitly supported in *Cotton* v. *The King*, where Lord Moulton held: 'There is no accepted principle in international law to the effect that nations should recognise or enforce the fiscal laws of foreign countries.'[102] But, equally, there is no principle of international law which prohibits such collaboration; States are free to help each other in the enforcement of their public law, and yet, they choose not to.

C. *Unilateral enforcement strategies*

Before further exploring the reasons for the lack of cooperation in respect of public law and resistance to it in respect of private law, one may ask what alternatives, if any, are open to States for imposing their regulatory will on foreign wrongdoers or, more generally, for upholding their local policies within their territories despite foreign violations. What can States do unilaterally, without having to rely on the help of other States? Apart from abandoning the traditional type of coercive State regulation in favour of self-help or self-regulation – which given the type of activities in question would often be unacceptable[103] – there are some strategies States have opted for in order to hold onto their traditional prohibitions.

Symbolic prosecution without enforcement

First of all, even when the foreign wrongdoer is not present, and has no assets against which a judgment could be enforced, in the State, a State may still decide to bring a prosecution against a foreign wrongdoer, as in Yahoo and the German *Töben* prosecution.[104] Such actions are of symbolic and 'educational' value: they signal to the world not just the content of the prohibition but also that the prohibition is taken seriously even in respect of foreign online publishers. They set an example which

State, but governments are also free to deny such effects by invoking their *ordre public*'. See also Jennings and Watts, above n. 45, 490.

[102] *Cotton* v. *The King* [1914] AC 176, 194.

[103] The criminalisation of these activities shows by itself that the State has made it a regulatory priority, vital for the community at large, and thus not even sufficiently addressed by the mere *ad hoc* nature of civil litigation.

[104] *Töben* (BGH, 12 December 2000, 1 StR 184/00, LG Mannheim) (2001) 8 *Neue Juristische Wochenschrift* 624; see the discussion in Chapter 4, section 4.C, above. Although, even in private cases, for example *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, where the private party carries the risk of unenforceability, a court's decision to allow the claim to go ahead still even though enforceability is unlikely, also signals the importance of a judgment *per se*.

is bound to deter some would-be wrongdoers. Where the State in question is popular as a business or tourist destination, foreign wrongdoers also face the risk of arrest on entry into the foreign State – which indeed occurs now and again.[105] However, such prosecutions are and must be exceptional; over-usage would, if anything, draw attention to the lack of real power of the law enforcers. Also, such prosecutions are likely to impress much more otherwise law-abiding online actors rather than online rogues.

Imposition of penalty on related local persons

Another enforcement option available at times is to seek to enforce a prohibition against a foreign wrongdoer by penalising a local person related to the wrongdoer. In Yahoo, LICRA had asked the Paris court to enforce the judgment against the US parent company by penalising Yahoo! Inc.'s French subsidiary.[106] The Paris court declined to do so.[107] This was a wise decision, as that approach is both doctrinally and practically problematic. Many foreign wrongdoers do not have a local subsidiary, and, even if they do, such as Yahoo! Inc., they would be penalised for their efforts to comply with local law. By using local subsidiaries as a lever to impose the regulatory will on the foreign parent, it would discourage the setting up of such subsidiaries and, by implication, legal compliance. Secondly, such actions would not be easily reconcilable with the concept of the separate personalities of companies, and would be contrary to the fundamental idea that criminal responsibility should attach to the actual wrongdoer.[108]

[105] Roy Mark, 'Feds Arrest Offshore Gambling CEO' (18 July 2006) Internetnew.com, www.internetnews.com/bus-news/article.php/3620731/.

[106] Complaint for Declaratory Relief, *Yahoo! Inc.* v. *LICRA*, No. C 00-21275 (PVT) (ND Cal., 21 December 2000), para. 29: the 'defendants asked the Paris Court to permit them to enforce against Yahoo! France any orders issued by the Court against Yahoo! Inc.'; for the denial by the Paris court, see para. 30(e).

[107] *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000). Note, under US law, this is not necessarily the case: see §414 of the US Restatement (Third) of Foreign Relations Law (1986).

[108] Vicarious liability and criminal liability are not generally understood to run easily together. '[I]t is desirable that criminal convictions be based on a showing of blameworthiness. The Latin maxim *nulla poene sine culpa* (no publishment without fault) expresses the idea that only defendants whose culpability has been demonstrated should be subject to criminal sanction': James Gobert and Maurice Punch, *Rethinking Corporate Crime* (London: Butterworths, 2003), 62. See also *Case Concerning the Barcelona Traction, Light and Power Company, Ltd (Belgium* v. *Spain*) (*Preliminary Objections)* [1964] ICJ Reports 6, where the ICJ looked to the nationality

Analogous prohibitions imposed on local intermediaries and end-users

Alternatively, States have sought to uphold their regulatory policies within their territories by targeting not, or not exclusively, the foreign online provider, but rather by imposing analogous or complementary prohibitions on local publishers, intermediaries and end-users. For example, in the EU the Data Protection Directive – which excludes non-EU actors with no equipment within the EU from its scope[109] – imposes on local controllers of personal data a duty not to transfer such data to any country where that data would not be adequately protected.[110] In the case of child pornography, local 'consumers', and not just online providers, commit a criminal offence by possessing the material in question.[111] In France, Article R-645-1 of the Penal Code bans the mere visualisation of Nazi-propaganda items and that would include downloading them onto a computer in France.[112] In the US, the UK and Australia, breaches of music copyright perpetrated via peer-to-peer file-sharing music websites have in recent years also been tackled by occasional, highly publicised actions against local small-time infringers rather than against the foreign facilitators of those breaches.[113] These prosecutions, primarily against teenagers, rely on a maximum amount of media exposure to scare.[114] In Italy, restrictions on offering gambling services are not only enforced against the local or foreign operators of those services, but equally against local intermediaries and local consumers of those illegal offers.[115]

of the company in form (the place of incorporation) rather than in substance (the location of its shareholders) to determine which State had *locus standi*.

[109] Art. 4 of the Data Protection Directive, 95/46/EC.

[110] Art. 25 of the Data Protection Directive, 95/46/EC.

[111] Art. 9 of the Council of Europe Cybercrime Convention (2001), which refers not only to making, offering and distributing child pornography but also to procuring and possessing it.

[112] *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000), where the Paris court stated: 'the mere visualisation in France of such objects constitutes a violation of article R-645-1 of the Penal Code.'

[113] Of course, the facilitators have also been subjected to prosecutions and private claims when they were present in the State. See the recent US Supreme Court decision against providers of peer-to-peer file-sharing software used on a gigantic scale for copyright infringement: *Metro-Goldwyn-Mayer Studios Inc.* v. *Grokster Ltd*, 545 US 125 (2005); Bobbie Johnson, 'US File-Sharing Judgment Will Net the Big Fish' (28 June 2005), *The Guardian*, http://arts.guardian.co.uk/netmusic/story/0,1516192,00.html.

[114] See also the notice on www.grokster.com.

[115] See *Criminal Proceedings against Piergiorgio Gambelli*, Case C-243/01, [2003] ECR I-13031, para. 9; Art. 4 of Law No. 401 of 13 December 1989.

In all these instances, foreign online activity which is illegal in the State is tackled through the imposition of obligations imposed on local actors. While there is no doubt that this has some impact on compliance, it often entails catching innumerable little fish, which is cost-intensive and lacks the efficiency inherent in tackling the big fish, i.e. the provider or facilitator of the illegal activity directly.[116] Furthermore, apart from relatively clear-cut cases like copyright infringement or possession of child pornography, it may simply be inappropriate to make the 'consumption' itself of illegal foreign products or services an offence. How would an online consumer know that a certain medication is unlicensed in his State? As for 'innocent' local intermediaries, it would often be too burdensome and generally undesirable to make them guardians against third party violations or, for that matter, the final arbiter of legitimate and illegitimate online speech. This explains why in both the EU and the US such intermediaries are largely immunised from liability for the content of third parties, foreign or otherwise.[117]

Prohibition of supportive services by local actors

Another option is to make the illegal foreign websites or the goods or services they offer less easily accessible from within the State.[118] One way of achieving this is not to prohibit them but to forbid local actors to advertise those services in any way, which is, as we saw, the strategy pursued in New Zealand with respect to foreign gambling services.[119] In the US, financial intermediaries have been pressured (through the threat of prosecutions) into denying credit card transactions with illegal

[116] Swire, above n. 4.

[117] Section 230 of the US Communications Decency Act (1996): 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.' Arts. 12–15 of the Electronic Commerce Directive, 2000/31/EC, making the liability of intermediaries dependent on the intermediary's control assumed over third-party content and its knowledge of the third-party violation. Mark Turner, 'Ignorance is Bliss' (2003) 19 *Computer Law and Security Report* 112.

[118] See the discussion in Chapter 3, section 3.A, above, on the similarity in, and differences between, accessibility of goods or services in the offline and online world.

[119] Section 16(1) of the Gambling Act 2003; for further discussion, see Chapter 5, n. 45, and the accompanying text. See also *People* v. *World Interactive Gaming Corp*., 714 NYS 2d 844, 851 (1999), relying *inter alia* on §225-05 of the New York Penal Code which prohibits the promotion of unlawful gambling activity.

foreign gambling enterprises.[120] These measures create practical hurdles which make non-compliance less likely although still possible.[121]

Blocking of foreign illegal content

While the above measures do not prevent access to foreign illegal sites, but rather make it more difficult to find and use them, the more radical method of protecting the local law space from being undermined by foreign breaches is to block any illegal foreign site, for example via local ISPs. As simple and straightforward as the idea may sound, given the vast number of sites, such blocking is associated with significant logistical problems in terms of both determining and blocking only the relevant sites.[122] Leaving those tasks to blocking software invariably leads to under- or over-blocking; the former fails in its purpose and the latter blocks out permissible speech.[123] But intelligent blocking software or not, ultimately it would be the government or private enterprises that would engage in censorship on a grand scale quite unprecedented in Western democratic States. Not surprisingly, authoritarian regimes, such as China, Cuba and Singapore, with long-standing censorship traditions, have had less hesitation in taking a no-nonsense approach to foreign online content considered undesirable or illegal.[124]

In summary, there is a host of unilateral legal measures at the disposal of States, and cumulatively they cannot but have some effect on ensuring greater legal compliance within their territories. Nevertheless, these

[120] For further discussion, see Chapter 5, n. 38, and the accompanying text; Christine Hurt, 'Regulating Public Morals and Private Market: Online Securities Trading, Internet Gambling and the Speculation Paradox' (2005) 86 *Boston University Law Review* 371.

[121] Of course, the same may be said about the offline world. The question is whether sufficient practical hurdles are created to discourage the activity in the vast majority of cases.

[122] For an early assessment of the blocking alternatives, see Commonwealth Scientific and Industrial Research Organisation (CSIRO) (Philip McCrea, Bob Smart, Marks Andrews), *Blocking Content on the Internet: A Technical Perspective* (June 1998), www.cmis.csiro.au/projects+sectors/blocking.pdf.

[123] For a case concerning the liability for over-blocking, see Laura Edgar, 'US – ISP – Immunity from Liability' (2005) 7 *Electronic Business Law* 14.

[124] Kristina M. Reed, 'From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce' (2000) 13 *Transnational Lawyer* 451; Shanthi Kalathil and Taylor C. Boas, 'The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution' (2001) Carnegie Endowment Working Papers, Global Policy Program No. 21, www.carnegieendowment.org/files/21KalathilBoas.pdf. More recently, Zhen Feng, 'China to Introduce New Legislation to Deal with ISP Liability for Copyright Infringement' (2004) 5 *World Internet Law Report* 19.

measures lack both the efficiency and the fairness of actions directed at the primary wrongdoers, and therefore are unsuitable to be employed across the regulatory board and thus are the preserve of high-priority regulation.

4. The public–private law dichotomy and its lessons for cooperation[125]

Why are States even in principle not willing to cooperate in the enforcement of each other's public law nor more tolerant of each other's legal differences in the enforcement of each other's private law – particularly given that more cooperation would be so beneficial? What lies behind the public–private law dichotomy that might explain the lack of, or resistance to, cooperation?

Below, it is argued that the public–private dichotomy embodies an evaluative ordering or spectrum of law. The relative position of a law, judgment or act on the public–private spectrum depends not on *what* activity the law seeks to regulate but on *who* is behind it, whether it is the State or a private individual. The greater a State's interest in the regulation of an activity, and the more it is designed to benefit the State, the more likely it will be that it is public. And this public status entails greater restrictions under public international law and not more, as common sense might suggest, but less cooperation by other States in its enforcement. The refusal by States to cooperate in the enforcement of foreign public law is not based on the potential harm the enforcing State may suffer as a result of the enforcement, but on the potential benefit gained by the foreign State. As astonishing as it may seem, foreign public law is not enforced, not *despite*

[125] Note that the terminology 'public' and 'private' is at times used to distinguish between publicly open parts of the Internet and privatised computer networks: Saskia Sassen, 'The Impact of the Internet on Sovereignty: Unfounded and Real Worries', in Christoph Engel and Kenneth H Keller (eds.), *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values* (Baden-Baden: Nomos, 2000), 195; Saskia Sassen, 'Digital Networks and Power', in Mike Featherstone and Scott Lash (eds.), *Spaces of Culture – City, Nation, World* (London: Sage Publications Ltd, 1999), 49. This discussion is not concerned with this understanding of the dichotomy. Neither is it concerned with the meaning of 'private' as describing the sphere which needs no law or regulation at all. Finally, the discussion also does not comment on the legitimacy of international private legislatures such as the Hague Conference on Private International Law or other private standard-setting agencies: see e.g. Antonio F. Perez, 'The International Recognition of Judgments: The Debate between Private and Public Law Solutions' (2001) 19 *Berkeley Journal of International Law* 44 or Henry H. Perritt, 'The Internet is Changing the Public International Legal System' (2000) 88 *Kentucky Law Journal* 885.

the fact that it would benefit the foreign State, but *because* it would do so. In other words, while States are ostensibly regretful about withholding cooperation, in reality they are not; rather, cooperation is withheld in order that the foreign State may not benefit from it.

A. 'Public' and 'private' international law

Although '[c]onceptions of public law and private law have never figured greatly in the history of the common law',[126] in the transnational legal context – common law tradition or not – the distinction exists simply by virtue of the respective ambits of private and public international law; indeed, their names reflect it.[127] Private international law supplies the competence rules for transnational disputes between private parties; in contrast, public international law – primarily concerned with the relationship of States *inter se* – delimits competence in respect of acts by States themselves when those acts affect other States.[128] Furthermore, the public law that is excluded from private international law is the very same public law that is the preoccupation of the competence regime of public international law. Such common definition can safely be assumed, given the complementary nature of these two bodies

[126] John Henry Merryman, 'The Public Law–Private Law Distinction in European and American Law' (1968) 17 *Journal of Public Law* 2, 19 and 18; cf.: 'Public law' and 'private law' are in civil law systems 'terms of legal art . . . [that] have been built into a systematic conceptual legal structure . . . [and] dominate the entire legal process.' Baade, above n. 80, 435f. The closest common law equivalent is the distinction between civil and criminal law; see *Atcheson* v. *Everitt* (1775) I Cowp 382, 391: 'there is no distinction better known that the distinction between civil and criminal law.'

[127] Note Kelsen, above n. 16, 245f: 'The terms "private" and "public" international law . . . seem to indicate an opposition within the international legal order, although public international law is simply international law, the adjective "public" being completely superfluous, while private international law is, at least normally, a set of norms of national law characterized by the subject-matter of legal regulation.' Generally on the relationship between these two bodies of law, see the extensive discussion by Mann (1971), above n. 2.

[128] Those acts may be judicial, legislative or executive, along the lines of the three branches of government. Bernard H. Oxman, 'Jurisdiction of States', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 277, 278. As noted above at n. 45, there is disagreement on the issue of whether the competence rules under public international law also concern themselves with private matters and private international law. Also, whether and to what extent the dichotomy as it exists in the domestic context overlaps with the public–private dichotomy which underlies jurisdictional questions in the transnational context is beyond the scope of this discussion.

of law[129] dealing with the same generic allocation issues.[130] This was expressly acknowledged by the US Supreme Court in *Huntington* v. *Attrill*: 'a statute of one State, which . . . is a penal law *in the international sense* . . . cannot be enforced in the courts of another state.'[131]

The ambits of private and public international law already indicate that the private or public nature of a law, judgment or act is not primarily dependent on *what* type of activity the law or judgment is concerned with, but rather on *who* is behind it: the State or a private individual. The same substantive prohibition can give rise to either a private or a public action or, in common law jargon, to a civil action or criminal prosecution. Furthermore, the public and private categories are not static or the same, regardless of the society and the perceived regulatory function of the State; they are dynamic, 'supplied with content by the culture of a given time and place'.[132] For example, gone are the days 'when private property, private wrongful conduct, and private contract were indeed separated intellectually, legally, sociologically, and in many ways, economically and politically, from the activities of the

[129] Strictly speaking, of course, there is no one body of private international law but as many bodies as there are national legal systems.

[130] On the common ancestry, see B. A. Wortley, 'The Interaction of Public and Private International Law Today' (1954) 85 *Recueil des Cours* 239, 247 (footnotes omitted): the 'law of nations' had historically 'comprised what is [today] called public international law and . . . conflict of laws'; Lowenfeld, above n. 75, 321: 'two branches . . . [that] have grown from the same tree'; but see also Hessel E. Yntema, 'The Historic Bases of Private International Law' (1953) 2 *American Journal of Comparative Law* 297; and more generally Michael C. Pryles, 'Internationalism in Australian Private International Law' (1989) 12 *Sydney Law Review 96*.

[131] *Huntington* v. *Attrill* 146 US 657, 673f (1892) (emphasis added). Similarly, on appeal, *Huntington* v. *Attrill* [1983] AC 150, 155, the Privy Council noted: 'Their Lordship cannot assent to the proposition that, in considering whether the present action was penal in such sense as to oust their jurisdiction, the Courts of Ontario were bound to pay absolute deference to any interpretation which might have been put upon the Statute of 1875 in the State of New York. They had to construe and apply an international rule.'

[132] Merryman, above n. 126, 15; on the changing perception of what ought to be considered 'private' or 'public', see Robert H. Mnookin, 'The Public/Private Dichotomy: Political Disagreement and Academic Repudiation' (1982) 130 *University of Pennsylvania Law Review* 1429, 1430: '[T]he very activities that are labelled private by liberal Democrats are considered public by conservative Republicans and vice versa. These differences can be dramatically exposed by asking for the dimension of the "public" and the "private" spheres in the realm of sexual expression and in the pursuit of economic goods.'

state'.[133] But not only has the State appropriated to itself areas of law traditionally considered within the private realm, traditional State functions have also been taken over by private powers: 'We live in a day when multinational and other huge agglomerations of so-called private power are tightly intermeshed at all levels with more traditional sovereigns.'[134] So the boundaries between the two categories are fluid. But when can a case no longer be considered private and becomes public? What are the definitions and underlying concerns of these categories in the transnational context? What triggers non-cooperation?

B. The public–private law spectrum

In *Yahoo*, the judges struggled with characterising the French order as either public or private and ended up with very different conclusions[135] – a fact which by itself foreshadows that the dichotomy defies simple definitions. The judgment most robustly in favour of the public character was that of Ferguson J, who argued that, despite the private form of the litigation, the judgment was public, an act of State, as it gave effect to the public interest of the French government.[136] According to Ferguson J, this was supported on three grounds: first, by reference to the plaintiffs, whom he classed as 'non-governmental, anti-racist associations and institutional partners with the French government in fighting anti-Semitism . . . [and who] followed the French government's mandate to enforce Le Nouveau Code Penal . . . a criminal provision . . . with the assistance of Mr Pierre Dillange, First Deputy Prosecutor'.[137] Secondly, it was supported by reference to the object of the law itself,

[133] P. B. Carter, 'Rejection of Foreign Law: Some Private International Law Inhibitions' (1984) 55 *British Yearbook of International Law* 111, 120f, citing Macneil, (1982–3) 7 *Canadian Business Law Journal* 432–3; Roscoe Pound, 'Public Law and Private Law' (1939) 24 *Cornell Law Quarterly* 469, 470f: 'public law is eating up private law . . . [T]he legal adjustment of relations involved in trade, finance, banking, industry, transportation, public utilities, and the like, are "a penetration of public law into the domain of private law"'; Mnookin, above n. 132, 1432: '[T]he trends of the last fifty years – both legislative and judicial – certainly suggest that the economic realm has generally come to be seen as more public'; Lowenfeld, above n. 75, 325, on the growth of public law.

[134] Carter, above n. 133, 120f.

[135] Apart from two of the three judges who dismissed for lack of personal jurisdiction, above n. 25.

[136] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1226 (9th Cir. 2006).

[137] *Ibid*., 1226f, but note the prosecutor never got involved in US litigation (*ibid*., 1204); also Ferguson J characterises the French orders as 'final criminal judgments' (*ibid*., 1227, n. 3).

which was designed to protect 'the collective memory of a country profoundly traumatized by the atrocities committed by and in the name of the criminal Nazi regime ... [preventing] a threat to the internal public order'.[138] The French judgment set forth 'the moral judgment of France itself'.[139] Thirdly, by reference to the wider State policy: the French order was part of the 'robust French state policy against racism, xenophobia, and anti-Semitism ... [and of the] efforts to criminalize racist speech within its borders'.[140]

In seemingly stark contrast, the minority held that the 'French lawsuits were civil rather than criminal and, more importantly ... the French orders primarily sought to redress a wrong to LICRA and UEJF rather than a wrong to the French public'.[141] That conclusion it supported, first, by reference to the nature of the plaintiffs being 'public interest, non-governmental organizations dedicated to defending the interests of certain victimised groups',[142] secondly, by reference to the actions being based on the New Code of Civil Procedure, thirdly, by reference to the nature of the award of damages to the plaintiffs by way of restitution, and, finally, by reference to the purpose of the penalties being to coerce Yahoo into compliance rather than to penalise it retroactively for a public wrong done.

Ferguson J's logic – that respect for the will of a foreign sovereign and its right to determine speech standards within its own borders demands judicial abstention,[143] i.e. non-cooperation – seems perverse; this abstention necessarily means that France cannot determine its speech standards within its own borders. By the same token, there is something disingenuous about the minority's holding that cooperation would have been forthcoming in this purely private case, were it not for the constitutional clash.[144] This is particularly so considering that constitutional rights are there to protect against *governmental* interferences, i.e. public interferences. In the transnational context, the governmental interference was that of the foreign sovereign.[145] Indeed, it seems that in

[138] *Ibid*., 1227. [139] *Ibid*., 1227. [140] *Ibid*., 1227.

[141] *Ibid*., 1248f, but the minority did not purport to express a final opinion on the matter as 'the issue has not been the focus of the parties' briefs or arguments' (*ibid*., 1248) and should thus 'be remanded to the district court for appropriate briefing and factfinding' (*ibid*., 1251).

[142] *Ibid*., 1249. [143] *Ibid*., 1228. [144] *Ibid*., 1250f.

[145] So a finding that there is a violation of the constitution presupposes an understanding of the interference as a public interference, either directly or indirectly. Houweling, above n 6, 701, where the author criticises the fact that 'the courts ... assume that mere

the final analysis the substantive concern giving rise to these ostensibly very different judgments[146] was one and the same: a foreign sovereign seeking to extend its governmental policy to a US national. Be that as it may, here are two judgments pointing in exactly opposite directions without either being blatantly wrong. The French case seems to have an equally distributed number of private and public indicia.

Given the decisive role of the public–private dichotomy in terms of the *prima facie* willingness to cooperate, it is curious how resistant to definition these terms have proven to be. While some definitions of public law as 'prerogative rights',[147] claims '*jure imperii*',[148] 'government interests'[149] or 'political law'[150] have been suggested, no definition has ever proved quite satisfactory or practicable. Mann summarises this oddity as follows:

> It would be of considerably greater value if it were possible to suggest an accurate and comprehensive definition of the rights which come within the scope of these descriptions. But at no stage of the historical development and in no country have lawyers succeeded in satisfactorily determining what is meant by 'public law' ... and what comes under the heading of 'private law' ... Yet the inability of the human mind and vocabulary to explain and contain cases by an all embracing form of words does not disprove the reality of a distinction which ... must be considered as indispensable.[151]

enforcement of a foreign speech-restrictive judgment has the same First Amendment ... implications as imposition of a speech-restrictive rule by a state actor in the first instance.'

146 The minority: private judgment but unenforceable on public policy grounds; Ferguson J: public judgment and therefore unenforceable.

147 Mann (1973), above n. 2, 499f.

148 *Ibid*.

149 *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 42: 'The expression "public laws" has no accepted meaning in our law ... It would be more apt to refer to "public interests" or, even better, "governmental interests" to signify that the rule applies to claims enforcing the interests of a foreign sovereign which arise from the exercise of certain powers peculiar to government.'

150 Mann (1971), above n. 2, 183, commenting on the definition of public law as 'political law' and its rejection in *Regazzoni* v. *K C Sethia (1944) Ltd* [1958] AC 301.

151 Mann (1973), above n. 2, 500; Jennings and Watts, above n. 45, 489: 'The distinction ... although very widely adopted in the present context and of undoubted value, is on analysis less easy to define than at first sight might appear'; Martin Davies, Sam Ricketson and Geoffrey Lindell, *Conflicts of Laws – Commentary and Materials* (Sydney: Butterworths, 1997), 233, referring to the 'inherent and treacherous difficulties associated with the distinction between private and public'; see also Carter, above n. 120, 120f.

The inability adequately to define private law and public law is due to the very nature of the dichotomy. It is superimposed upon what is in fact a spectrum of laws or judgments, reflecting a continuum of interests. At one end of the spectrum the State takes a clear and manifest regulatory interest in a particular activity; at the other it is up to a private individual to seek redress, with the middle ground being occupied by cases like *Yahoo*. There is no pre-existing dichotomy of cases but only a spectrum,[152] and the ambiguities on the boundary cases are an unavoidable consequence of a legal polarisation of a continuum of cases.

The dichotomy reflects the regulatory decision to cooperate in respect of cases at one end of the spectrum, but not the other.[153] The definition of public law by Lowenfeld, as 'the kind of law that would not ... be applied (directly or under a judgment) by the court of another State',[154] is correct. To say that foreign public laws are unenforceable is a tautology.[155] Asserting that a case is public is the legal conclusion, and thus can provide little assistance in determining whether the law is enforceable or not. This seems to underlie the dissatisfaction with the private–public dichotomy as an analytical tool,[156] as well as the resistance of common law systems to the dichotomy itself and their preference for

[152] It illustrates the tendency of law, in the name of certainty and predictability, to favour categories over an undivided spectrum. While substantively in respect of all foreign law it may be more accurate to ask whether there are any public policy grounds for or against its enforcement, greater certainty and predictability is achieved by creating divisions such as non-enforceable penal or revenue law, on the one hand, and enforceable contract or torts law on the other. Yet, no matter how valuable, the creation of these categories comes at a price, which lies in their inevitably blurred boundaries, and these categories thus themselves give rise to some uncertainty.

[153] This seems to support the argument that the private–public dichotomy has quite different meanings in different contexts.

[154] Lowenfeld, above n. 75, 324; Mann (1973), above n. 2, 492f.

[155] For this reason, to argue that some foreign public law should be enforced simple does not makes sense, as labelling of a law as the 'public' of necessity means that it is non-enforceable. *AG of New Zealand* v. *Ortiz* [1982] QB 349, 371: 'The kinds of law which would be comprised in such a wide class are so many and so various, that some should properly be enforced in this country while others perhaps should not', correctly rejected on appeal: *AG of New Zealand* v. *Ortiz* [1984] AC 1. Mann (1971) above n 2, 116, where the author starts his discussion of public law by stating that '[n]o attempt will be made to define public law'.

[156] H. Lauterbach, 'The Problem of Jurisdictional Immunities of Foreign States' (1951) 28 *British Yearbook of International Law* 220, 240, where the author notes that the distinction between acts *jure gestionis* and acts *jure imperii* has 'proved to be impracticable and productive of uncertainty'.

narrower categories such as penal or revenue laws that avoid the even wider and looser boundaries of the public-law category.

The problematic cases are those that occupy the middle ground. Their classification can only partly be informed by comparison with the cases which fall within the far ends of the spectrum, precisely because they are not like the clearly public or clearly private cases. By analogy, if one had a big-egg/little-egg dichotomy to impose different prices, what would happen to the medium-sized egg? As it is neither big nor little, its categorisation into one or the other group would not precede the analysis of whether it ought to be big or little, but is its outcome. Comparison to the big or little eggs would offer guidance with respect to some eggs, but would fail in the very middle ground where the similarity to the big eggs or little eggs would be equal. There, the classification would depend on an evaluation of whether one could get away with selling the medium-sized egg at the higher price, i.e. by an evaluation of the consequences flowing from the classification.[157] In other words, the potential outcome drives the classification. The final classification of the medium-sized egg as big or little is identical to its consequence, namely, that it is sold at the higher or the lower price.

Because the classification of the middle-ground cases, like *Yahoo*, cannot but be done by reference to its consequences, i.e. should one cooperate or not, the seemingly drastic difference in principle between Ferguson J and the minority is theoretical gloss. On the consequences they clearly agreed: no cooperation. Perhaps even theoretically their principled differences are more apparent than real. In *AG of New Zealand* v. *Ortiz*, Staughton J argued that the question which should be addressed in respect of all foreign law is not whether a law is public or private, but 'whether there is any special ground of public policy which requires the law in question not to be enforced here'.[158] The idea – that *all* foreign law held not to be enforceable, is not enforced on public-policy grounds, also has some academic support: 'a wide range of choice of law rules operate as judicially created substitutes for public policy . . .

[157] Another alternative, according to my son, would be not to sell them at all and eat them.

[158] Although he appears to limit the validity of this test to public law cases which are neither penal nor revenue cases. *AG of New Zealand* v. *Ortiz* [1982] QB 349, 371. He further attempts to extend this rule in reverse to certain public matters, by saying that they should be enforced if the forum's public policy demands it, which seems a logical extension of an understanding of the 'public policy' exception as providing answers for the middle-ground between the clearly unenforceable foreign public law and the clearly enforceable foreign private law. See also *Lorentzen* v. *Lydden & Co. Ltd* [1942] 2 KB 202.

Among these substitutes, and crystallising into concrete rules, would be included: non-recognition of penal and revenue laws.'[159]

The upshot is that with cases like *Yahoo* it is to be expected that judges will disagree on whether it is an unenforceable private case or a necessarily unenforceable public one, as they are neither quite public nor quite private,[160] but occupy the 'unenforceable' middle-ground. In the end, the theoretical differences often conceal the same substantive concerns, and certainly are of no practical significance. It must be doubted whether LICRA or France care too much about whether the case was private or public. This brings us to the final question: what makes one case enforceable but not the other, or what are the criteria which give rise to the ordering of cases along the private–public spectrum? For this purpose, it is instructive to examine when and why a case falls into the public category.

C. Underlying concern: foreign State interest and involvement

Few would dispute Lenin's comment that '[a]ll law is, of course, public'.[161] Even private law fulfils a public function and is for the good of the community at large: 'If it were not, the application of private law would not be entrusted to organs of the State.'[162] Yet States have shown a willingness to cooperate in respect of some private laws. The above discussion already foreshadows that it is the extent of the foreign State's involvement and substantive interest in a case which makes it

[159] Holder, above n. 74, 929; see also Mann (1971), above n. 2, 183: 'it may well be that some and perhaps all of the decisions which proclaim the maxim could have been founded upon the demands of public policy.'

[160] In *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, the judges, although coming to the same conclusion, differed in their view on whether the foreign law was not enforceable on the ground that it sought to protect a foreign public interest or on the ground that it was a private cause of action but the enforcement of which was contrary to the public policy of the forum.

[161] Lowenfeld, above n. 75, 21; Merryman, above n. 126, 11f, where the author explains the ideological background of the claims that 'all law is public law', on the one hand, and 'all [bourgeois] law is private law' on the other hand.

[162] Kelsen, above n. 16, 207; see also *Huntington* v. *Attrill* [1893] AC 150, 157: 'All the provisions of Municipal Statutes for the regulation of trade and trading companies are presumably enacted in the interest and for the benefit of the community at large; and persons who violate these provisions are, in a certain sense, offenders against the State law, as well as against individuals who may be injured by their misconduct. But foreign tribunals do not regard violations of statute law as offences against the State.'

more or less public. But how exactly is that involvement or interest measured?

In *Yahoo*, the judges, in deciding on the public or private nature of the case, placed – to varying extents – reliance, first, on the character of the plaintiffs,[163] secondly, on the legal basis of the action (i.e. the civil code versus criminal code) and its wider purpose,[164] and, thirdly, on the character of the final order and its intended beneficiaries.[165] This approach sits squarely with the interrelated criteria that emerge from the body of case law: *who* brings the actions, *whose* cause of action is it (i.e. whose prerogative is it to bring the action) and *who* is intended to benefit from the remedy?[166] These inquiries, it is submitted, reveal the extent of the foreign State's interest and involvement in the regulation of an activity. In clear-cut cases, all indicators point in the same direction: the State enforces the law in the particular instance and generally has the prerogative to do so, with the benefit of the final order flowing to the State. A clearly private law is one which is not only enforced by a private individual in the particular instance, but typically enforceable by private individuals who seek reparation or compensation for their loss or damage sustained. In cases like Yahoo, the criteria point in opposite directions.

Also typically, in *Yahoo* the judges emphasised that it is the substance that matters and not the form. For example: 'the label "civil" does not strip a remedy of its penal nature.'[167] Along the same lines, the High Court of Australia in *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd*

[163] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1219 (the majority), 1226f (Ferguson J), 1249 (the minority) (9th Cir. 2006).

[164] *Ibid*., 1219 (the majority), 1227 (Ferguson J), 1248f (the minority).

[165] *Ibid*., 1220 (majority), 1250 (minority).

[166] Similar criteria were considered determinative in respect of the substantive scope of the Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters: see Hague Conference of Private International Law (Peter Nygh and Fausto Pocar), *Report of the Special Commission*, Prel. Doc. No. 11 (1999), 35f: 'Paragraph 3 . . . further clarifies the meaning of "civil and commercial matters". The characterisation of the claim cannot be made to depend merely on whether a government . . . or any other person acting for the State is a party . . . [T]he Convention will apply to disputes involving government parties, if the dispute contains the following core criteria: the conduct upon which the claim is based is conduct in which a private person can engage; the injury alleged is injury which can be sustained by a private person; the relief requested is of a type available to private persons seeking a remedy for the same injury as the result of the same conduct.'

[167] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1219 (the majority), 1249 (the minority) (9th Cir. 2006).

stated that 'for the purposes of the principle of unenforceability under consideration the action is to be characterized by reference to the substance of the interest sought to be enforced, rather than the form of action'.[168] Such comments do not undermine the validity of the above three indicators, but rather confirm their relevance in principle and in the vast majority of clear-cut cases. The search for the 'true' substance is the only way to solve those hard cases where the inquiries point in opposite directions; it is to iron out the inconsistencies and squeeze the case in one of the categories.

Public versus private complainants

The standard case is simple: there are no 'offences against the State, unless their vindication rests with the State itself . . . [or with] an official duly authorised to prosecute on its behalf'.[169] If the complainant is the State or its nominee, then the law is *prima facie* unenforceable. So, in *Raulin* v. *Fischer*,[170] which concerned a civil intervention by an injured

[168] *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 46; see also *US* v. *Inkley* [1989] 1 QB 255, 265: 'the fact that in the foreign jurisdiction recourse may be had in a civil forum to enforce the right will not necessarily affect the true nature of the right being enforced in this country'; and *Huntington* v. *Attrill* [1893] AC 150, 155. Mann (1971), above n. 2, 176f. Similar comments in respect of competence rules under international law have been expressed by Akehurst, above n. 2, 146: 'An act by one State in the territory of another is forbidden . . . if it is, *by its nature*, an act which only officials of the local State are entitled to perform, as opposed to an act which private individuals can perform. For instance, collecting taxes is something which can be done only by public officials, not by private individuals' (emphasis added).

[169] *Huntington* v. *Attrill* [1893] AC 150, 158f; see also *Ayres* v. *Evans* (1981) 56 FLR 335, 337, where Fox J stated that the non-enforcement rule applies to cases 'where the revenue authority, or some person acting in its interest or on its behalf, seeks to enforce the revenue liability as such'.

[170] *Raulin* v. *Fischer* [1911] 2 KB 93, even though there was only one judgment in this case. Similarly, Akehurst, above n 2, 191, argued in the context of US anti-trust regulation: 'For the purpose of determining the limits of jurisdiction permitted by international law, it is submitted that a suit by the injured party is similar to a private action in tort for damages, and that a suit by the Department of Justice is similar to a criminal prosecution. In form a suit by the Department of Justice resembles a suit by the injured party, but in substance it is a public prosecution . . . for vindication of public right and for redress and prevention of public injury. The Department of Justice is not subject to the rules which limit the *locus standi* of private plaintiffs and some of the orders . . . are orders which would never be made in proceedings brought by a private party.' See also Hannah L. Buxbaum, 'The Private Attorney General in a Global Age: Public Interests in Private International Antitrust Litigation' (2001) 26 *Yale Journal of International Law* 219, 261, where the author notes that the court in one of the antitrust cases viewed 'the direct involvement of the UK government in the litigation' as an indicator of the 'public' nature of the dispute.

party in a criminal prosecution, Hamilton J held that the judgment in favour of the private party, unlike the prosecution, was enforceable.

The importance of the public or private character of the complainant is more obvious where it clashes with the nature of the cause of action. In *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd*,[171] the cause of action was a private one: breach of the duty of confidence and an employment contract. Yet the action was brought by the UK government, pursuing its governmental interest: 'to concentrate on the private law character of the causes of action . . . is to overlook the appellant's central interest in bringing the action. That interest is to ensure the continued secrecy of the operation of the British Security Service.'[172] Having said that, a private case brought by the State does not always entail non-enforcement as even States can have rights and obligations under private law: 'In all modern legal orders, the State . . . may have rights *in rem* and rights *in personam*, nay any of the rights and duties stipulated by "private law" . . . The fact that a legal relationship has the State for one of its parties does not necessarily remove it from the domain of private law.'[173] Nevertheless, a review of a cross-selection of cases suggests that for enforcement purposes the odds are stacked highly against States, even when they claim to be acting in their private capacity.[174]

While the participation of States in litigation tends to give a 'public' colour to even private causes of action, it rarely works in the reverse. When private individuals purport to enforce what is in fact 'public law', the case thereby does not become 'private'. In *Peter Buchanan Ltd and Macharg* v. *McVey*,[175] the Irish Supreme Court did not allow the claim

[171] (1988) 165 CLR 30.

[172] *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 46.

[173] Kelsen, above n. 16, 202. Note Carter, above n. 133, 117: '[I]n modern times the State, and organs of the State, have become involved in a wide and diverse range of day-to-day commercial, quasi-commercial, and social activities – from the fact that, for example, State or local authority provision of services in return for direct or semi-direct payment has become commonplace.' On the law governing contracts between States and foreign private person, see Mann (1990), above n. 2, Chapter 9. See also *Kunstsammlung zu Weimar* v. *Elicofon*, 536 F Supp 829 (EDNY 1981), affirmed in 678 F 2d 1150 (2nd Cir. 1982) and *Williams & Humbert* v. *W & H Trade Marks* [1986] 2 WLR 25.

[174] Not enforceable: *Government of India* v. *Taylor* [1955] AC 493; *United States* v. *Harden* (1963) 41 DLR (2d) 721; *Brokaw* v. *Seatrain UK Ltd* [1971] 2 QB 476 (where the US government was brought in as claimant through an interpleader summons); *AG of New Zealand* v. *Ortiz* [1984] AC 1; *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30. Contrast: *Huntington* v. *Attrill* [1893] AC 150; *Connor* v. *Connor* [1974] 1 NZLR 632; *Ayres* v. *Evans* (1981) 56 FLR 335.

[175] [1955] AC 516.

by the liquidator of a Scottish company to recover moneys from the company's shareholder, as the whole purpose of the action was to collect a foreign tax: 'The foreign revenue instead of courting certain defeat by suing here in its own capacity resorts to bankruptcy proceedings ... to enforce his claim here.'[176] Such cases are relatively clear-cut public cases, comparable to those cases where a 'member of the public ... [pursues what] is regarded as an actio popularis ... not in his individual interest, but in the interest of the whole community'.[177] It becomes more complicated when some private redress is sought in addition to defending the 'public good'.[178] In cases where the government purposefully creates private remedies to encourage private litigation to complement State enforcement the pendulum swings back to the public side: 'A private litigant acts as a private attorney general if the litigant asserts a cause of action not only to obtain compensation, but also to vindicate important public interests ... [encouraged] by statutory mechanisms.'[179]

In *Yahoo*, most of the judges categorised the two anti-racist organisations as private litigants; after all, they were non-governmental organisations.[180] The minority emphasised that the plaintiffs were 'dedicated to defending the interests of members of certain victimised groups',[181] implicitly stressing that their activities were not for the public good at large but rather for identifiable groups of private beneficiaries. Yet, there is also some force in Ferguson J's argument that the organisations were in fact 'institutional partners with the French government in fighting anti-Semitism'.[182] Take in addition the fact that they 'litigated with the assistance of Mr Pierre Dillange ... representing the office of the Public Prosecutor',[183] and the public cloud casting its shadow over the litigation is unmistakable. Yet, as a typical boundary case the arguments are rather inconclusive.

Public versus private cause of action

In many ways the public or private nature of the complainant informs the search for the 'true' nature of the cause of action, a matter equally beset with difficulty in the middle-ground. In principle, the question is

[176] *Peter Buchanan Ltd and Macharg* v. *McVey* [1955] AC 516, 530.
[177] *Huntington* v. *Attrill* [1893] AC 150, 158. [178] *Ayers* v. *Evans* (1981) 56 FLR 335.
[179] Buxbaum, above n. 170, 233 (internal footnotes omitted).
[180] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1219 (the majority), 1248f (the minority) (9th Cir. 2006).
[181] *Yahoo! Inc.* v. *LICRA & UEJF* 433 F 3d 1199, 1249 (9th Cir. 2006).
[182] *Ibid*., 1226. [183] *Ibid*., 1227.

whether the action is one 'in the nature of a suit in favour of the State'.[184] Unenforceable foreign laws are those which are *in their nature* enforceable by the State (regardless of who actually enforces them in the particular case), such as penal and revenue laws, exchange-control and export-restriction as well as confiscatory legislation.[185] 'The rule applies to claims enforcing the interests of a foreign sovereign which arise from the exercise of certain powers *peculiar* to government.'[186] And these are not powers peculiar to any government, but those which the government in the particular State has specifically made its own.[187]

Again, sometimes, even though the claim is brought by the government or one of its agencies, the apparent and real cause of action is held not to be peculiar to the government.[188] In *Weir* v. *Lohr*,[189] the Canadian Health Insurance Commission was successful in enforcing an outstanding debt on the hospital accounts, as it was in substance a private contractual claim. Yet, more typically, the reverse occurs: private causes of action, such as a property, contractual or tortious claim,[190] are held to disguise what are in fact public actions, particularly where the State is the litigant. In *United States of America* v. *Inkley*, the civil suit on an appearance bond was in fact held to be designed 'to ensure, so far as it was possible, the presence of the executor of the bond to meet justice at the hands of the state in a criminal prosecution'.[191] In *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd*, the civil action masked 'an

[184] *Huntington* v. *Attrill* [1893] AC 150, 157. [185] Mann (1971), above n. 2, 172.

[186] *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 42 (emphasis added), criticised by Mann (1990), above n. 2, 358f. See Akehurst, above n. 2, 146ff, where the author refers to these as acts which can by their nature only be done by public officials, such as the collection of taxes.

[187] A few causes of actions are universally considered peculiar to government, such as tax claims.

[188] *Kunstsammlung zu Weimar* v. *Elicofon*, 536 F Supp 829 (EDNY 1981), affirmed 678 F 2d 1150 (2nd Cir. 1982).

[189] (1967) 65 DLR (2d) 717; but contrast *Municipal Council of Sydney* v. *Bull* [1909] 1 KB 7, where the council failed to recover a contribution in return for improvements made to the street where the defendant owned property, as the claim was in substance held to be a tax claim; discussed in Michael Mann, 'Foreign Revenue Laws and the English Conflict of Laws' (1954) 8 *International and Comparative Law Quarterly* 465, 467ff.

[190] *Huntington* v. *Attrill* [1893] AC 150, 156: 'no proceeding, even in the shape of a civil suit, which has for its object the enforcement by the State, whether directly or indirectly, of punishment imposed for such breaches of lex fori, ought to be admitted in the Courts of any other country.' For example, *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30 (contract and duty of confidence) and *Bank voor Handel en Sheepvaart NV* v. *Slatford* [1953] 1 QB 248 (conversion).

[191] *US* v. *Inkley* [1989] 1 QB 255, 265.

exercise of a prerogative of the Crown, that exercise being the maintenance of national security'.[192]

The issue becomes more thorny where ostensibly private litigants rely on an ostensibly private cause of action, as in Yahoo. The nature of the cause of action in Yahoo was as ambiguous as the character of the plaintiffs. Although in form a civil claim, substantively it was based on a 'manifest' breach of the French Criminal Code. Which one should count? It is not uncommon for activity that gives rise to a potential criminal offence also to found a civil cause of action. Often though, the civil claim follows, or goes hand in hand with, the criminal prosecution, as it did in *Raulin* v. *Fischer*.[193] In such cases, the civil claim is there to provide a private remedy to the injured party and no more. But where, as in Yahoo, there is no earlier or concurrent prosecution, even though the facts of the case would clearly have warranted one,[194] the civil case may well be regarded as a substitute for a criminal prosecution. Indeed, there is evidence from US antitrust proceedings that the absence of a parallel criminal prosecution clearly influences the course and outcome of the private case:

> [F]luctuations in enforcement patterns reveal similar shifts in the focus on public and private values. During periods in which a larger percentage of private lawsuits are 'follow-ons' to public enforcement actions, the private value of compensating the victim takes precedence over the public deterrent value; conversely, when more private suits are initiated independent of government action, the emphasis is on the public role of the litigant in bringing to light antitrust violations that would not otherwise have been prosecuted.[195]

[192] *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 46. For a further German case, see Mann (1984), above n. 2, 43f.

[193] [1911] 2 KB 93. See, for example, UK Protection from Harassment Act 1997 which in addition to creating the offence of harassment also provides for a civil remedy to the injured party (s.3).

[194] A prosecution was subsequently started against Yahoo! Inc. and its ex-CEO, Timothy Koogle: *R* v. *Timothy K and Yahoo Inc.* (Tribunal de Grande Instance de Paris, 26 February 2002, No. 0104305259), www.foruminternet.org/telechargement/documents/tgi-par20020226.pdf. It appears that the complaint by the Organisation for Prisoners of Auschwitz and Concentration Camps was filed in February 2001, after which the prosecution was initiated. Koogle was subsequently cleared of all charges: *R* v. *Timothy K and Yahoo Inc.* (Court of Appeal in Paris, 11 February 2003), affirmed in *R* v. *Timothy K and Yahoo Inc.* (Court of Appeal in Paris, 6 April 2005); see 'Ex-Yahoo! CEO's Nazi Auction Acquittal Upheld in France' (7 April 2005), OUT-LAW.COM, www.out-law.com/page-5510/.

[195] Buxbaum, above n. 170, 224f (footnotes omitted); see also Salil K. Mehra, 'Deterrence: The Private Remedy and International Antitrust Cases' (2002) 40 *Columbia Journal of Transnational Law* 275. This also makes Akehurst's proposition, above n. 170, that

In the circumstances, it can be assumed that the Paris court treated the Yahoo case not just as simply a private suit for the benefit of LICRA with no higher public function. This would explain the involvement of the French prosecutor. Also, Gomez J's comments abundantly confirm the public aspect: 'an offence against the collective memory of a country profoundly wounded by the atrocities committed by . . . the Nazi criminal enterprise against its citizens'[196] and 'a threat to the internal public order'.[197] As Ferguson J said, the French court 'gave clear effect to the collective efforts of French civil liberties organizations, the French government, and French law enforcement to enforce French criminal provisions'.[198] That this 'civil action' was not merely or primarily designed to compensate LICRA for its injuries is also confirmed by the final orders – which too were made against the background of the non-existent criminal prosecution.

Public versus private remedy

Again, the character of the final order is designed to illuminate the real nature of the cause of action. In *Huntington* v. *Attrill*, the US Supreme Court noted: 'The prosecution was in the name of the state, and *the whole penalty, when recovered, would accrue to the state*.'[199] However, just because a remedy 'bears no relation to the actual loss or damage sustained by the party to whom the action is given . . . [or] inflicted upon grounds of public policy'[200] does not entail its public status. So a public or penal order is not simply any order which is 'penal in the wider sense

antitrust actions should be classified as private, if brought by private litigants, problematic.

196 *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000).

197 *Ibid*.

198 *Yahoo! Inc*. v. *LICRA and UEJF*, 433 F 3d 1199, 1227 (9th Cir. 2006).

199 *Huntington* v. *Attrill*, 146 US 657, 672 (1892) (emphasis added). In *Government of India* v. *Taylor* [1955] AC 491, 506, the leading case on the exclusion of foreign revenue law, the House of Lords said: 'upon the assumption which must be made, that the decision in *Huntington* v. *Attrill* was correct, it was conceded that it must cover not only penalties strictly so-called but also any tax which could be regarded as penal or confiscatory.'

200 *Huntington* v. *Attrill* [1893] AC 150, 153, but note 156: 'the expression "penal" and "penalty", . . . are calculated to mislead, because they are capable of being construed so as to extend the rule to all proceedings for the recovery of penalties, whether exigible by the State in the interest of the community, or by private persons in their own interest'; see also Hague Conference on Private International Law, above n. 166, 31: 'Likewise, the fact that the damages awarded are exemplary or punitive does not deprive the proceedings of a civil or commercial character, as long as the benefit of those damages

in which the term is used ... [including penalties that] are in their nature protective and remedial'.[201] Mann has suggested that the order must be 'an exercise of governmental might providing a monetary imposition for the benefit of the State. Emphasis must be placed upon the involuntary nature of the imposition ... for no objection has been made to foreign governments recovering a contract debt.'[202] But that test fails to explain why compulsory quasi-contractual payments due to the State for services rendered have been held enforceable.[203] If, on the other hand, one focuses on the party to whom the remedy flows (i.e. the State or a private individual), one again enters troubled waters: exemplary damages are enforceable,[204] but treble damages awards provided for by US anti-trust legislation are not.[205] Both of these payments – penal in the wider sense rather than compensatory – are recoverable by private litigants. The real difference, it is submitted, is that the availability of

goes to the plaintiff and not to the State.' But note Carter, above n. 133, 114: 'Whether a law is penal depends primarily upon its purpose. The principal criterion is as to whether the main thrust of the law is the infliction of punishment at the instance of, or on behalf of, the State, or is the award of compensation.'

201 *Huntington* v. *Attrill* [1893] AC 150, 159.

202 M. Mann, above n. 189, 466. But problematic again are cases like *Ayers* v. *Evans* (1981) 56 FLR 335, where not all, but only some of the award was due to the foreign revenue authorities.

203 *Weir* v. *Lohr* (1967) 65 DLR (2d) 717. In *US* v. *Ivey* (1996) 139 DLR (4th) 570, a Canadian court held that the US government was entitled to recover the expenses for remedial measures undertaken by the US Environmental Protection Agency on the defendant's waste-disposal site.

204 *SA Consortium General Textiles* v. *Sun and Sand Agencies Ltd* [1978] QB 279, 299f. But see also §483, Comment b, of the US Restatement (Third) of Foreign Relations Law (1986): 'Some states consider judgments penal for purposes of non-recognition if multiple punitive, or exemplary damages are awarded, even when no governmental agency is a party.' Cited in *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1220 (9th Cir. 2006).

205 *British Airways Board* v. *Laker Airways Ltd* [1984] 1 QB 142, 163: 'Parliament has said that if judgment is recovered in that action it will not be enforced here. Parliament has also said that the defendants, if they pay under any such action, shall be entitled to recover back the penal element from the plaintiff.' See also Foreign Antitrust Judgments (Restriction of Enforcement) Act 1979 (Cth) which stipulates that, where an order has been made under that Act prohibiting the enforcement of a foreign antitrust judgment, an Australian defendant may take proceedings in Australia to recover from the foreign plaintiff any amount which has been recovered under that foreign antitrust judgment, including the non-punitive first third of treble damages. See also Commonwealth of Australia, *Australia–United States Relations: The Extraterritorial Application of United States Laws*, Joint Committee on Foreign Affairs and Defence (Canberra, 1983), 14: 'The treble damages remedy is penal in its purpose and effect.'

treble damages awards is meant to provide an incentive for private parties to take over the enforcement of anti-trust law and thereby relieve the burden upon the State:

> A private litigant acts as a private attorney general if the litigant asserts a cause of action not only to obtain compensation, but also to vindicate an important public interest ... [encouraged by] statutory mechanisms, such as fee shifting, that are implemented to promote litigation. The goal of developing such mechanisms, and thereby encouraging private litigation, is to deter unlawful behavior by supplementing the government resources devoted to enforcement.[206]

In contrast, the availability of exemplary damages is not designed to encourage private litigation to supplement government resources, but is just a deterrent device.[207] The general conclusion cannot but mirror those above: if a payment is recoverable by the State it is not necessarily public, but there is a strong presumption to that effect. If, on the other hand, an order is for the private party and that order is penal rather than strictly compensatory, it is a public order where there is evidence that the State uses the private litigation to complement its own actions and that, in turn, depends on the broader regulatory context of the activity in question.

In *Yahoo*, there was significant disagreement on the nature of the penalty that backed the injunction and whether it was 'remedial in nature, affording a private remedy to an injured person, or penal in nature, punishing an offence against the public justice'.[208] So what was the purpose of the penalty? The majority viewed the penalty as public, that is, as a measure designed to 'deter conduct that constitutes a threat to the public order',[209] and emphasised its size in contrast to the

[206] Buxbaum, above n. 170, 223f (footnotes omitted), where the author also notes that private attorney-generals are used in a number of areas, beyond the antitrust context, such as environmental law and securities regulation. Furthermore, the requirement that the injury suffered must be of the type the antitrust laws are designed to prevent and not be too remote from the antitrust violation alleged, seeks to weed out cases that serve only the private goal of the litigant. Commonwealth of Australia, above n. 205, 14: 'Private antitrust suits serve to supply an ancillary force of private investigators to supplement the Department of Justice's law enforcement.'

[207] John G. Fleming, *The Law of Torts* (9th edn, Sydney: LBC Information Services, 1998), 271f: '"exemplary or punitive" damages focus not on injury to the plaintiff but on outrageous conduct of the defendant, so as to warrant an additional sum, by way of penalty, to express the public's indignation and need for deterrence or retribution.'

[208] *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1220 (9th Cir. 2006), citing *Ducharme* v. *Hunnewell*, 411 Mass 711, 714 (1992).

[209] *Yahoo! Inc.* v. *LICRA and UEJF* 433 F 3d 1199, 1220 (9th Cir. 2006).

nominal damages awarded to LICRA. The minority, on the other hand, argued that the damages awarded showed that the suit was civil, and that the injunction 'was merely an additional remedy' and the fines for non-compliance were simply meant to coerce Yahoo! Inc. into compliance with the injunction.[210] This latter reasoning is persuasive in so far as the character of the penalty for non-compliance with the injunction was not disconnected from the character of the injunction itself. However, to say that the injunction was merely an additional remedy to the nominal damages seems bizarre given the size of the penalty and the effort the French court went to to show that the injunction could be limited to its territory – hardly indications to show its insignificance. It seems the minority de-emphasised the injunction as it was the part of the remedy which would be for the benefit of the whole community, rather than the plaintiffs specifically. In the end, each judgment emphasised those parts of the orders which supported their final conclusion, with neither seeming conclusively wrong. The broader regulatory context though, as examined by Ferguson J, suggests that the purpose of the injunction (and implicitly of the penalty) was not merely remedial for the benefit of select private beneficiaries, but an integral part of France's 'dramatic efforts to criminalize racist speech within its borders'.[211] It would appear that LICRA stepped into the regulatory shoes of the State.

The paradox

As argued above, the wrangling about the public–private nature of the *Yahoo* case was theoretical gloss. None of the eleven judges held that the French order was enforceable, and six expressly rejected it – private or public character aside. Nevertheless, the examination of the private–public dichotomy incontrovertibly reveals that the more a foreign State itself is behind the action, and the more it is designed to discharge the regulatory role the foreign State has taken upon itself, the less likely it will be that cooperation by another State will be forthcoming: 'it is precisely in those spheres where a State has the greatest interest in having its law enforced by foreign courts ... that its law is least likely to be enforced.'[212] It is *because* a law or a case benefits the foreign State itself, that it will not be enforced.[213] The question is always: who will benefit

[210] *Ibid*., 1249f. [211] *Ibid*., 1227. [212] Akehurst, above n. 2, 221, and also 235.

[213] For small inroads, see cases such as *Foster* v. *Driscoll* [1929] 1 KB 470, where a contract that broke the laws of a friendly foreign country was not enforced. In *Regazzoni* v. *K C*

from cooperation. '[T]he category of the right of action, i.e. whether public or private, will depend *on the party in whose favour it is created*.'[214] This conclusion in all its simplicity is startling. One might have expected uncooperativeness to be connected with the substance of the foreign law, but clearly that is not the case: 'Why is it unlawful in Canada to evade local taxes and yet perfectly legitimate to refuse to pay foreign taxes? How can the public policy of Canada be invoked to protect tax dodgers when our own legislative bodies impose similar taxes?'[215] Or one might have expected that non-cooperation is based on the harm the enforcing State may suffer as a result of enforcement. But the occasions when the enforcing State could be said to be harmed by the enforcement, or to directly benefit from the non-enforcement, seem rare indeed. Unusually, in *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd*, the High Court of Australia concluded that the 'material concerning the operations of the British Security Service ... might well sustain a finding that the publication is in the Australian public interest'.[216] In the Yahoo scenario, the enforcement of the French order was unlikely to harm the US or its speech, unless of course any additional foreign regulatory burden is treated as harmful. What though is clear is that non-cooperation has an harmful effect overall on all States.[217]

It is beyond the ambit of this book to search for the reasons why States (and not just their judiciaries) are unwilling to act in a way which would be beneficial to other States – even where reciprocity could be agreed upon, and thus where the enforcing State would be guaranteed to benefit from its own cooperation in due course.[218] The most obvious reason

Sethia (1944) Ltd [1958] AC 301, the House of Lords refused to enforce a contract which required the doing of an act which required the commission of a crime in a foreign State.

[214] *US* v. *Inkley* [1989] 1 QB 255, 265 (emphasis added).

[215] Carter, above n. 120, 117, citing with approval Castel, *Canadian Conflict of Laws* (1975), Vol. 1, 64. See also *Williams and Humbert Ltd* v. *W & H Trade Marks (Jersey) Ltd* [1986] AC 368, 428.

[216] *AG (UK)* v. *Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30, 44f.

[217] It certainly is harmful to States collectively, as it encourages the evasion of tax and penal laws as well as other regulatory laws. A. R. Albrecht, 'The Enforcement of Taxation under International Law' (1953) 30 *British Yearbook of International Law* 454, where the author argues against the non-enforcement rule in respect of taxation; but note Baade, above n. 80, 497.

[218] To the author's knowledge, there are no treaties providing for the reciprocal enforcement of foreign public law.

would appear to be, what one commentator called, a 'rather jealous competition'[219] between States. If one further considers that the public status of a regulation reflects a decision to dedicate scarce governmental resources to its systematic enforcement,[220] competitiveness between States would dictate not expending one's own resources on furthering a foreign regulatory priority. Recent developments in the European Union would suggest that significant legal, economic and political integration is a necessary precursor to a loosening of the uncooperative stance.[221]

[219] Steinberger, above n. 1, 400; Buxbaum, above n. 170, 263: 'The way in which countries compete for regulatory control over international commerce, however, is highly nationalistic'; Baade, above n. 80, 497: 'Nevertheless, two considerations militate against the judicial enforcement of foreign-country tax claims . . . First, history has shown that revenue laws have been used for religious and racial discrimination; for the furtherance of social policies and ideals dangerous to the security of adjacent countries; and for the direct furtherance of economic warfare' (internal marks omitted); Niall Ferguson, *The Cash Nexus: Money and Power in the Modern World 1700–2000* (London: Allen Lane, 2001), 26f: 'money at the immediate disposal of the state treasury is usually more limited than the costs of war; and the history of finance is largely the history of attempts to close that gap . . . After many centuries during which the cost of warfare was the biggest influence on state budgets that role was usurped in the second half of the twentieth century by the cost of welfare.'

[220] Making an activity the regulatory concern of the State rather than private individuals may also be desirable where no specific individual is 'sufficiently' harmed by the generally harmful activity to create an incentive for private litigation.

[221] For an early inroad into the public-law taboo within the EC, see Convention between the Member States of the European Communities on the Enforcement of Foreign Criminal Sentences (1991). A cornerstone in this development was the Treaty of Amsterdam on the European Union (1999) which officially states that the creation of a common area of freedom, security and justice is an aim of the EU. See Programme of Measures to Implement the Principle of Mututal Recognition of Decisions in Criminal Matters (OJ C12/10, 2001), which followed the Tampere European Council in 1999 where it was decided that 'mutual recognition should become the cornerstone of judicial cooperation in both civil and criminal matters'. For an overview, see http://ec.europa.eu/justice_home/fsj/criminal/recognition/fsj_criminal_recognition_en.htm and http://ec.europa.eu/justice_home/fsj/criminal/fsj_criminal_intro_en.htm or http://europa.eu/scadplus/leg/en/s22006.htm. For a more recent development, see Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties (OJ L78, 22.3.2005). But see also European Commission, *Communication on the Mutual Recognition of Judicial Decisions in Criminal Matters and the Strengthening of Mutual Trust between Member States*, COM(2005) 195 final, http://europa.eu/scadplus/leg/en/lvb/l16001.htm, where the Commission notes that, even within the EU, Member States are still reluctant to recognise criminal decisions made in another Member State.

5. The future of cooperation

What does this entail for the future of cooperation in the online context? The message which emerges from the above discussion is not encouraging. Certainly, there is little to suggest that in the near future States will agree to a cooperative regime of the kind suggested by Lessig in *Code and Other Laws of Cyberspace*, according to which States would enter into pacts whereby one 'state would promise to enforce on servers within its jurisdiction the regulations of other states for citizens from those other states, in exchange for having its own regulations enforced in other jurisdictions'.[222] At the moment, the competence regimes institutionally enshrine non-cooperation in respect of those legal areas in which the foreign State takes a keen regulatory interest. Given that this stance has survived unscathed despite severe challenges posed by globalisation prior to the advent of the Internet, it would seem highly optimistic to expect any softening of this position in the near future.[223] The good-neighbour clauses as adopted in the Australian and UK online gambling legislation are bound to remain the exception and not the rule. However, a step in the right direction would be more extensive academic and governmental engagement with the non-cooperation rule and its basis in light of the modern tightly interconnected world. Perhaps too an engagement with the more general insights gained on the evolution of cooperation between competitive actors,[224] and how those insights may be applied to the non-cooperation rule, might finally lead to a gradual erosion of the non-cooperation stance in public matters.

If one cannot place one's bets on greater cooperation to compensate for the fact that 'the reach of the police officer is only as long as his arm',[225] one is left with the above-mentioned unilateral enforcement strategies with all their imperfections. Another option, albeit equally beset with difficulty, would be greater substantive legal harmonisation. As noted above, substantive legal harmonisation gets around much of the enforcement dilemma, as the enforcement action of each State over

[222] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 55. The good-neighbour clauses adopted in Australia and Great Britain in the online transnational gambling context present significant departures from the traditional non-cooperative position but have so far not been utilised, see Chapter 5, section 3.B, above.

[223] But note Baade, above n. 80, 494ff, where the author is more optimistic as to the likely future cooperation between States in respect of their public laws.

[224] See Axelrod, above n. 42.

[225] Lombois, above n. 3.

local wrongdoers indirectly ensures compliance with foreign laws as well. Moreover, given that the strict territorial limits of enforcement jurisdiction, coupled with the uncooperativeness of States, means that much foreign online activity escapes effective State regulation, there is currently significant bottom-up legal harmonisation. Or, put another way, States are in respect of much activity left with no choice but to tolerate the worldwide lowest common regulatory denominator. It is still possible to view and acquire Nazi memorabilia in France, and, even if a US court had agreed to enforce the French order, the chances are that there are other 'tolerant' States.

A preferable option to accepting this default bottom-up harmonisation would appear to be a negotiated compromise. But, even assuming it could be achieved, what are the costs, if any, of legal harmonisation? This is one of the questions considered in the final chapter of this book.

7

A 'simple' choice: more global law or a less global Internet

1. The hidden choice

The central question addressed in this book is: how can the transnational Internet be reconciled with national law? The preceding chapters have examined how courts and legislatures of various States have in various legal contexts worked with, rather than against, the national-law paradigm in dealing with transnational online disputes and events. The general picture which emerges is that national law has survived, and can survive, however uncomfortably, the online challenge. The solutions may not be perfect. However, a moderate country-of-destination approach goes quite some way towards striking a compromise between the perceived need of States to protect their local law space, on the one hand, and the need to protect online actors from overregulation and the openness of cyberspace, on the other hand. If in addition States could be persuaded to cooperate more extensively in the enforcement of each other's claims or/and perfect their unilateral enforcement strategies, national law and the transnational Internet are both accommodated, perhaps in an uneasy union, but reconciled in any event. Or are they?

This chapter pulls the cloth from underneath the discussion in the preceding chapters (if indeed it was there) and from the jurisdictional Internet debate more generally, by rejecting the idea that the transnational Internet and national law are reconcilable. They are not; they are logically irreconcilable, and thus practically so. It is impossible to hold onto national law successfully and not compromise the transnational openness of the Internet. It is as impossible as squeezing a size 14 person into a size 8 jacket. Either the person has to become slimmer or the jacket has to become bigger, or a bit of both. What is not doable is to make the size 14 person fit into the size 8 jacket, with both person and jacket remaining unchanged. And that is exactly the position with respect to the transnational Internet and national law: the transnational Internet and national laws can only be 'reconciled' either by creating a less

transnational Internet or more global laws or a bit of both. The globalisation of laws allows the Internet to be retained as an open medium but occurs at the expense of peculiar national laws and values. On the other hand, making the Internet less transnational, through territorial zoning of online activity, allows national policies reflecting peculiar cultural, social and political values to be preserved but at the expense of the uninhibited freedom of *transnational* online communications. Neither option is without drawbacks.

To assert this inherent irreconcilability is not to say that the arguments made in previous chapters are in any way invalid, but rather to highlight that, whatever regulatory solution to competence problems one favours – no matter how 'moderate', 'balanced' or 'fair' it may appear – there is always a price to be paid. You cannot have your cake and eat it. There is no ideal solution which allows for freedom of online communication *and* the preservation of national laws at the same time. A choice has to be made. First and foremost, that choice has to be made, and always is made, by States, but, as the discussion below shows, private actors are often also confronted with it.

Sometimes the irreconcilability and resultant choice shines through the literature on competence, but perhaps not as brightly as it should.[1] Typically, in *Dow Jones* v. *Gutnick*, Kirby J spelled out the consequences of imposing local defamation law on foreign publishers:

> The law in different jurisdictions, reflecting local legal and cultural norms, commonly strikes different balances between rights to information and expression and the protection of individual reputation . . . To tell a person uploading potentially defamatory material onto a website that such conduct will render that person potentially liable to proceedings in courts of every legal jurisdiction . . . may have undesirable consequences.

[1] For some notable exceptions within the secondary literature on the topic, see Yulia A. Timofeeva, 'Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis' (2005) 20 *Connecticut Journal of International Law* 199; Jonathan Zittrain, 'Be Careful What You Ask for: Reconciling a Global Internet and Local Law', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net*? (Washington DC: Cato Institute, 2003), 13; Jonathan Zittrain, 'Perspective: Can the Internet Survive Filtering?' (23 July 2002) Cato Institute, http://news.com.com/2010-1071-945690.html; Dan Jerker B. Svantesson, 'Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet' (2004) 23 *John Marshall Journal of Computer and Informational Law* 101; Dan Jerker B. Svantesson, 'Borders *on*, or Border *around* – The Future of the Internet' (2006) 16 *Albany Law Journal of Science and Technology* 343.

> Depending on the publisher and the place of its assets, it might freeze publication or *censor it* or *try to restrict access to it in certain countries*.[2]

And yet the court did precisely that: despite the undesirable consequences, it told Dow Jones that it was liable under Australian defamation law. The reason for that was that the undesirable consequences of *not* applying Australian defamation law seemed even worse; effectively it would have spelled the end of the Australian defamation law, being subsumed by the lower US speech standards.[3]

Sometimes that choice is completely hidden in liberal rhetoric. For example, the Council of Europe's Declaration on Freedom of Communication on the Internet (2003)[4] is explicitly committed to free online communications and yet its very first Principle on 'Content rules for the Internet' states that 'Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery'.[5] But it is precisely this application of existing law to online activity that threatens free transnational online

[2] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56, para. 117 (Kirby J) (emphasis added), discussed in depth in Chapter 4.

[3] *Ibid*., para. 115 (Kirby J): 'Any suggestion that there can be no effective remedy for the tort of defamation . . . committed by the use of the Internet (or that such wrongs must simply be tolerated as the price to be paid for the advantages of the medium) is self-evidently unacceptable.'

[4] Adopted by the Committee of Ministers on 28 May 2003; see also Council of Europe, *Declaration on Freedom of Political Debate in the Media* (adopted by the Committee of Ministers on 12 February 2004). See also Organization for Security and Co-operation in Europe (OSCE), *Amsterdam Recommendations on Freedom of the Media and the Internet* (2003). In the US context, see William J. Clinton, Presidential Directive on Electronic Commerce (1 July 1997), www.technology.gov/digeconomy/presiden.htm: 'For electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation . . . Parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. Therefore, the Federal Government should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or taxes and tariffs on commercial activities that take place on the Internet.' Although the rhetoric of self-regulation and a hands-off approach is contradicted by the innumerable attempts by States to apply their laws to the Internet, it still carries a certain sway: see e.g. Christian Ahlert, 'Technologies of Control: How Code Controls Communication', in OSCE (Christiane Hardy and Christian Möller), *Spreading the Word on the Internet* (Vienna: OSCE, 2003), 119. On the pretence of privatisation and a self-regulation in the ICANN context, see Harold Feld, 'Structured to Fail: ICANN and the Privatisation Experiment', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net?* (Washington DC: Cato Institute, 2003), 333.

[5] Note, Draft Declaration on Freedom of Communication on the Internet (8 April 2002), www.humanrights.coe.int/Media/documents/Draftdeclaration.rtf, Principle 1, which expresses the commitment to free communication, is in the final version only

communication. Indeed, in all of the examples discussed in previous chapters, States have 'only' tried to extend existing law to the Internet, rather than imposed 'restrictions which go further' than existing ones. The argument in this chapter is that it is impossible to hold effectively onto traditional national legal standards and, at the same time, maintain freedom of communications – despite fine Declarations to the contrary.

Transnational online communications versus national law – is there indeed only this choice and, if so, how is one to choose? These two questions are examined below and these are the broad conclusions: first, despite the seeming great variety of 'solutions' adopted or proposed to handle online transnationality in various legal contexts, they ultimately all fall within either of the above options. Similarly, any default position arising from failed 'solutions' falls within one of the two options. Secondly, making a choice comes down to a policy decision or a value judgment. Legal arguments may inform that decision but cannot conclusively solve it. For example, the limits of enforcement jurisdiction may often dictate against attempting to hold onto local law. Policy-makers (including judges, who are policy-makers of sorts[6]) have to decide what is more important: free uninhibited access to the global net or the retention and protection of local legal standards? Thirdly, the answer to that question can, and often does, differ in relation to different regulatory activity. A State may opt for more open online communications in respect of a certain type of regulated activity and for a more aggressive protection of national law in respect of another. The future regulation of the Internet and national legal spaces will be, and should be, a mixture of both, and this is already apparent, although rather diffusely, in current regulatory solutions. Finally, although many commentaries suggest otherwise,[7] more global law in the form of substantive global harmonisation is neither always ideal nor generally favoured. There are

Principle 3 which provides: 'public authorities should not through general measures, including measures such as filtering, deny access by the public to information and other communications on the Internet, regardless of frontiers. Neither should intermediaries, such as service providers, exercise or be obliged to exercise prior control of content which does not emanate from them'; and is then also qualified: 'measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.'

[6] See Chapter 2 on the breadth of the judicial discretion generally and in the online regulatory context more specifically, and the considerations that feed into its exercise.

[7] See, for example, Paul Schiff Berman, 'The Globalisation of Jurisdiction' (2002) 151 *University of Pennsylvania Law Review* 311, 392ff; Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10

good reasons why national law comes in all shapes and sizes, reflecting the peculiar political, cultural and social values of States and their communities, and those reasons which gave rise to different laws in the first place still often militate against harmonisation of laws in the online era.

The arguments made in this final chapter are, where appropriate, illustrated by reference to the regulation of spam, although – like in the preceding chapters – they are by no means peculiar to it. Spam presents a suitable example for the question examined here, because it is an all-pervasive problem that has affected all States. Unsolicited email has plagued the online environment since the early commercial days of the Internet, and presents a problem for businesses, individuals and the online community generally:

> Spam clogs up corporate networks, slowing down legitimate traffic and forcing businesses to deploy anti-spam software or let their users waste hours deleting the messages. Spam cost European companies €2.4bn (£1.7bn) in lost productivity last year, by some estimates. It is not just businesses that hate spam: individuals also have to wade through e-mail in-boxes filled with junk and worry about their children being bombarded with unsavoury messages from pornographers.[8]

Today, spam is also often used for sinister purposes, such as financial cons and delivering worms, viruses and Trojan horses. Yet, despite the universality of the spam problem, and its persistence, it has – like much, but not all, universally deplored online activity – not benefited from a globally harmonised solution.[9] It seems that the chances of successful legal harmonisation, even in respect of, what may be labelled, 'morally

International Journal of Law and Technology 139, 176; Karsten Bremer, *Strafbare Internet-Inhalte in International Hinsicht – Ist der Nationalstaat wirklich überholt*? (Frankfurt a. M.: Peter Lang Verlag, 2001), http://ub-dok.uni-trier.de/diss/diss60/20000927/20000927.pdf, 176ff; Graham J. H. Smith (ed.), *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002), 517ff; Denis T. Rice, '2001: A Cyberspace Odyssey Through US and EU Internet Jurisdiction Over E-Commerce' (2001) 661 *PLI/Pat* 421, 453.

[8] Fiona Harvey, 'E-Marketing in a Straitjacket' (2 December 2003), *Financial Times*, 16, http://search.ft.com/search/article.html?id=031202000787/. Note that, in 2005, spam still accounted for two-thirds of all emails: UK Office of Fair Trading, *Cross-Border Action to Tackle Spam* (3 November 2005), www.oft.gov.uk/News/Press+releases/2005/208-05.htm. See also Hazel Raw, 'Spam: Where's the Beef?' (2004) 15(1) *Computers and Law* 38; 'Bill Gates Death-of-Spam Prediction Flops, as "Dirty Dozen" Spam Countries Revealed' (23 January 2006), Sophos, www.sophos.com/pressoffice/news/articles/2006/01/dirtdozjan05.html.

[9] The Organisation for Economic Co-operation and Development (OECD) and the International Telecommunication Union (ITU) have been particularly active in fostering cooperation in the fight against spam; note in particular OECD Spam Task Force, *Anti-Spam Regulation* (2005) DSTI/CP/ICCP/SPAM(2005)10/FINAL, www.oecd.org/dataoecd/29/12/35670414.pdf, 29f (on cross-border issues); ITU, *ITU*

neutral' regulatory agendas (in contrast to issues such as hate speech, as examined in Chapter 6) are rather slim. Furthermore, spam is also an activity particularly suited to regulation through private 'technological' measures, and thus perhaps not in need of State interference. Yet States have interfered and opted for different solutions,[10] but what are the consequences of these attempts? Also, spam provides a good legal context, as it shows that the arguments previously made in respect of websites are relatively easily transferable to other Internet activity, such as email. Finally, as spam may be considered a new regulatory field with only distant predecessors,[11] its regulation has not been 'burdened' by the regulatory baggage of its predecessors. This has also meant that the regulation of spam can be restricted to the online world, with less pressure for it to conform to the regulation of comparable offline activity. In other words, policy-makers have had a relatively free hand in tackling it and as clean a regulatory slate to write upon as any. And still, despite this best-case scenario, States have not adopted regulatory policies that would protect freedom of transnational communications. Let us now turn to the two essential options open to deal with the inherent conflict between the transnational Internet and national law.

2. More global law

Substantive harmonisation is often advocated as the only truly viable solution to the inadequacies of national law in respect of transnational online activity: 'After all, if a universal substantive law were applied

Survey on Anti-Spam Legislation Worldwide (2005) CYB/06, www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. There are a number of Memoranda of Understanding and Joint Statements concerning the regulation of spam and providing for a commitment to cooperation, e.g. between Australia and Korea, Thailand, the UK, the US and Canada, www.dcita.gov.au/communications_and_technology/policy_and_legislation/spam/spam_international. See also the London Action Plan on International Spam Enforcement Cooperation (February 2005), www.londonactionplan.com.

[10] For a comprehensive survey of anti-spam legislation worldwide, see ITU, www.itu.int/osg/spu/spam/ as well as report on the survey, above n. 9.

[11] One such predecessor is ordinary junk mail, which is within the EU subject to an opt-out rule, in contrast to the opt-in rule adopted in respect of spam. Junk mail raises different problems, as shines through Recital 42 of the Directive on Privacy and Electronic Communications, 2002/58/EC: 'Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephone calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls.'

around the world, many of the concerns about borders, conflicting law, and impermissible extraterritorial regulation would disappear.'[12] The arguments in favour of harmonisation are powerful. If online activity pays no respect to State boundaries, then by definition law ought also to transcend boundaries to be effective. More specifically, from the perspective of State regulators, globally harmonised legal standards would mean that they would no longer need to 'fight' illegal foreign content infiltrating their regulatory space.[13] The enforcement action of each regulator taken against locally established wrongdoers would also indirectly benefit foreign regulators. From the perspective of online actors, harmonisation would be ideal as only one legal standard, rather than currently a multitude of diverging national standards, would govern their activity, no matter where the online activity originates or takes effect. This would make it easy to foresee, know and comply with legal obligations. From the perspective of the online community generally, border-crossing communications would no longer be tainted and discouraged by the legal uncertainties arising from entering different national spaces and the fear of potential liability under hostile foreign laws. Global or harmonised law simply means that there is no need to superimpose national boundaries onto cyberspace with all the consequences that entails. The questions which will be considered now are: what forms can this harmonisation take and why does it remain an elusive goal, apart from a few isolated exceptions?

A. Harmonisation of competence rules?

The type of harmonisation which caters for the transnational openness of the Internet is harmonisation of substantive law, rather than harmonisation of competence rules such as championed by the Hague Conference on Private International Law, although the latter is likely to be a more achievable target.[14] No doubt, the latter would also be

[12] Berman, above n. 7, 392; see also other literature listed above n. 7.

[13] This assumes that each State takes its regulatory responsibility seriously, an assumption which is not always justified.

[14] Holger P. Hestermeyer, 'Personal Jurisdiction for Internet Torts: Towards an International Solution?' (2006) 26 *Northwestern Journal of International Law and Business* 267, 286ff, arguing for a convention endorsing the targeting test for online torts; Richard Garnett, 'Regulating Foreign-Based Internet Content: A Jurisdictional Perspective' (2000) 6 *University of New South Wales Law Journal* 8, www.austlii.edu.au/au/journals/UNSWLJ/2000/8.html, 1, noting that a treaty on choice-of-law rules would

beneficial; it would make it easier for online actors to predict with certainty when a particular national law becomes relevant and avoid some conflicting claims by different States.[15] However, the harmonisation of competence rules would significantly reduce neither the regulatory burden of online actors nor the difficulties faced by regulators in respect of illegal foreign content.[16] Online actors would, and should, remain alert to the possibility of being sued or prosecuted under, and in, numerous foreign regimes, and take measures to protect themselves against such exposure. Regulators would, and should, take measures to instil that alertness in foreign online actors, and to do whatever else is within their powers in order to protect their local legal patch. Competence rules presuppose and protect diverse national legal spaces rather than whitewash them.[17] In other words, competence rules, harmonised or otherwise, have the exact opposite purpose to harmonisation of substantive law: they preserve, rather than deny, legal diversity amongst States.

There appears to be a critical difference between competence rules determining the applicable law and those laying down which court has jurisdiction to hear a dispute. Any rule determining whether this substantive law or that should govern a dispute clearly presupposes that the substantive laws under consideration are different. Otherwise, there is nothing to choose. But this does not necessarily hold true for

be more realistic than the harmonisation of substantive law. Despite this, the efforts of the Hague Conference on Private International Law to comprehensively harmonise the law on adjudicative jurisdiction have failed: see Kurt Wimmer, 'International Liability for Internet Content: Publish Locally, Defend Globally', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net*? (Washington DC: Cato Institute, 2003), 239, 258ff; see also Berman, above n. 7; 395.

[15] It would create greater legal certainty for online actors who could more accurately predict their potential legal exposure and take actions to avoid it. They would not need to be over-cautious and prevent entirely 'harmless' contacts, as currently fostered by the lack of transparency of the plethora of private international law bodies.

[16] For a contrary view, see Timofeeva, above n. 1, 223ff. Note also, better enforcement could be facilitated if mutual enforcement and recognition of foreign judgments were to be part of the harmonisation of competence rules, as was planned in respect of the proposed treaty by the Hague Conference on Private International Law.

[17] As the purpose of competence rules is to delimit the application of one set of regulation *vis-à-vis* other sets, if there is complete harmonisation there is only one set of regulation that applies without limits. Ulrich Magnus and Peter Mankowski, *Joint Response to the Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument and its Modernisation COM(2002) 654 final* (2003), 2, http://ec.europa.eu/justice_home/news/consulting_public/rome_i/news_summary_rome1_en.htm, on the diminishing rationale for conflict-of-law rules with increasing harmonisation in the context of EU contract law.

adjudicative jurisdiction rules: it is possible (and almost invariably the case[18]) that harmonised substantive law is administered through various national courts. Diversity in adjudication does not seem irreconcilable with harmonisation of substantive law.[19] By the same token, and returning to the general argument of this chapter, the retention of national courts does not seem to stand in the way of uninhibited global online communications – as long as those courts apply the same substantive law. In the discussion here, the broad accuracy of this proposition is assumed, at least to the extent to which it is argued that *more* global law, even if not truly global law, can be created through harmonised national law administered through national courts.

Having said that, two observations are apt at this point. First, many of the decisions considered in preceding chapters concerned the jurisdiction of the court rather than choice of law. Yet still, they have caused substantial concern within the online community and certainly encouraged the adoption of precautionary 'territorial' measures by online providers – thus they *have* contributed towards chilling transnational online communications and superimposed national borders on cyberspace. Admittedly, in these cases the applicable law was not harmonised and admittedly, too, the assumption of adjudicative jurisdiction often has an impact on which substantive law is applied.[20] Nevertheless, it is highly unlikely that substantive legal harmonisation would alleviate all the concerns of online providers and spell the end of their precautionary territorial measures. While it may be as easy to communicate and transact online with a person from the UK as with one from Chile or Japan, it is not as equally easy to defend a suit in the UK, Chile or Japan – harmonised substantive law or not. As long as the practical burden arising from a dispute is greater in respect of a foreign customer (or

[18] Notable exceptions e.g. the International Court of Justice, the European Court of Justice and the European Court of Human Rights.

[19] This is only partly true as the adjudication by State courts – bound hand and foot with different legal traditions and following different procedures – often means that, despite harmonised substantive law, there are marked differences in its application. The reception of public international law or EC law within domestic law has been subject to much scrutiny; see, for example, Gerrit Betlem and Andre Nollkaemper, 'Giving Effect to Public International Law and European Community Law before Domestic Courts: A Comparative Analysis of the Practice of Consistent Interpretation' (2003) 14 *European Journal of International Law* 567.

[20] See, for example, Chapter 4, section 1, above in the defamation context. On the less obvious homeward trend, see Michael Akehurst, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145, 185.

business) than a local one, all things are not equal with respect to foreign and local customers (or businesses). So the system of diverse national courts adjudicating transnational online dispute presents in itself a disincentive to transnational online activity.

Secondly, while adjudication appears to be a 'neutral process', in fact adjudicative processes and procedural laws vary as widely as applicable substantive laws, and reflect and protect – just like substantive laws – the peculiar, deeply ingrained values of each State.[21] It is trite to say that substantive laws without adequate procedural processes and safeguards would more often than not miss their target. Ultimately, procedural laws and processes are no more 'neutral' than substantive laws, and the former is an integral adjunct to the latter. Although adjudication by different States is not as overtly irreconcilable with uninhibited transnational communications, in fact once it is understood as part and parcel of each distinct legal regime, national adjudication is as irreconcilable with the transnational openness of the Internet as are national *substantive* laws.

The general point is that competence rules, whether dealing with substantive law or procedural law/processes, harmonised or not, presuppose and protect legal diversity amongst States. The existence of competence rules necessarily implies, first, that choices can be made between this law or court or that law or court and, secondly, that the choice is significant, i.e. it has consequences for the parties or States concerned. In contrast, with complete legal harmonisation these differences are non-existent. No matter where the activity occurs and who are the parties to the dispute, the same rules, substantive or procedural, apply; the location of the activity or the parties and their link with any particular State is irrelevant for legal purposes. Only under those latter conditions would national legal borders truly no longer exert pressure on the transnationality of online activity, and vice versa. But then national borders would be superfluous.

B. Substantive harmonisation by design

Substantive legal harmonisation by design can occur in essentially two ways: at the higher level, or at the lower level. Either States come to a

[21] This is reflected, for example, in the fact that enforcement of a foreign judgment may be denied on the basis of misgiving about the foreign adjudicative process: see e.g. §482(1)(a) of the US Restatement (Third) of Foreign Relations Law (1986): 'A court in the United States may not recognize a judgment of the court of a foreign state if (a) the judgment was rendered under a judicial system that does not provide impartial tribunals or procedures compatible with due process of law.'

consensus at a higher supranational level or they come to a consensus by surrendering regulation to the 'lower' private level, allowing private players and institutions to take over. In the latter case, harmonisation occurs through deregulation, that is, through regulation other than in its conventional State-centric and location-centric form.[22]

Harmonisation through treaty

The Internet era has witnessed some harmonisation success stories at the higher supranational level. In respect of private contract law there are two UNCITRAL Model Laws and a Convention,[23] and in respect of public/criminal law there is the Council of Europe Cybercrime Convention (2001).[24] What seems astonishing is the speed with which these have been agreed upon. Yet, on closer inspection, it seems that consensus could be reached in these cases quickly simply because it was already substantially there, at least with respect to the general moral merit or depravity of the activities in question and the mode of regulating them.[25] For example, the Cybercrime Convention 'codifies' rather than truly harmonises at international level a limited number of criminal offences. Matters where genuinely new harmonisation could have occurred, such as the legal status of hate speech, did not make it into the Convention.[26] So the Internet era has not created a legal environment

[22] The discussion touches upon, but cannot do justice to, the substantial debate on the changing multi-level and overlapping sources of regulation in the global context: see e.g. Chris Harding, 'The Identity of European Law: Mapping Out the European Legal Space' (2000) 6 *European Law Journal* 128 (commenting on the fragmented and multi-layered model of ordering in the EU context); Neil MacCormick, 'Beyond the Sovereign State' (1993) 56 *Modern Law Review* 1; Peter Thomas Muchlinski, 'Globalisation and Legal Research' (2003) 37 *International Lawyer* 221, 229f (noting the 'de-centering [of] national law . . . downwards through an increasing localisation of legal activity through principles of subsidiarity or devolution . . . [and] upwards towards delocalisations of legal activity through supranational regulation').

[23] UN Convention on the Use of Electronic Communications in International Contracts (2005), Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001).

[24] The Convention entered into force on 1 July 2004. Goodman and Brenner, above n. 7, 188ff; Indira Carr and Katherine S. Williams, 'Cyber-crime and the Council of Europe: Reflections on a Draft Convention' (2001) 4 *International Trade Law and Regulation* 93.

[25] Goodman and Brenner, above n. 7, 177ff, noting that crimes against the person and crimes against property are consensus crimes, that is, similar in all States. Even crimes against the State, e.g. treason, are in essence comparable, unlike, however, crimes against morality where there are significant differences between national laws.

[26] Council of Europe's Additional Protocol to the Cybercrime Convention, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through

where deep-seated cultural and political differences are easily overcome – despite the repercussions of not finding a common bottom-line. Certainly, lofty notions such as the need to preserve the Internet as an open transnational communication medium have had little to do with harmonisation. The preamble to the Cybercrime Convention refers to 'the need to ensure a proper balance between the interest of law enforcement and . . . the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, *regardless of frontiers*'.[27] However, given the nature of the acts outlawed, such as hacking and child pornography, it can safely be assumed that the freedom to communicate child pornography 'regardless of frontiers' weighed little in the balance. The driving force behind the Convention was the desire for effective law enforcement. In respect of universally criminalised activities, there is simply no conflict between preserving national legal diversity and preserving the Internet as a globally open communication medium – because legal diversity is negligible and free communication not desired. On the other hand, the desire to preserve the transnational openness of the Internet clearly does explain the drive for harmonisation in the private contractual context, where 'uniform rules [are designed] to remove obstacles to the use of electronic communications in international contract'.[28] The rules harmonised in this context tend to have a decidedly facilitative, rather than prescriptive, character,[29] designed to encourage generally endorsed activity. So the desire to retain the openness of the Internet falls onto a very specific and particularly fruitful legal ground. But how much force does it exert beyond this narrow area?

The real problems start when one goes beyond the narrow core of activities that are universally condemned or endorsed. When it comes to gambling, banking, trading in securities or other economic activity, or hate, political, religious, pornographic, privacy-encroaching or

Computer Systems (adopted by the Committee of Ministers on 7 November 2002, in force since 1 March 2006). Note, initially it was thought possible to accommodate hate speech within the Cybercrime Convention: 'Council of Europe Cyber-Crime Treaty Attacked by ISPs' (2001) 4 *World Internet Law Report* 33, 34. Laura Leets, 'Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace?' (2001) 6 *Communication Law and Policy* 287.

[27] Council of Europe's Cybercrime Convention (2001), para. 10 (emphasis added).

[28] Preamble to UN Convention on the Use of Electronic Communications in International Contracts (2005).

[29] Matters covered are designed to clarify how concepts of traditional contract law apply to electronic contracts, such as the time and place of offer and acceptance, and to ensure the validity of electronic contracts.

reputation-damaging 'speech' – there is much diversity in how States deal with these activities legally.[30] Regulation that would be in the eyes of one State an undue encroachment on the freedom to communicate is in the eyes of another a legitimate curb on that freedom. Substantive harmonisation has not occurred even where the difference of opinion seems rather slight, which is by no means unusual. Most States agree in principle that consumers deserve some protection in their dealings with businesses or that children should be shielded from pornographic material. But variations in the detail of how much protection there should be and how it should be implemented,[31] and perhaps an inherent resistance to making an external legal commitment, have prevented States from finding a common denominator.

Harmonisation through deregulation

Another way in which law can be globalised is through deregulation, that is, the substantial withdrawal of the State from the regulatory agenda. This type of regulatory approach has had many advocates, especially in the early days, and often goes along the lines of Johnson and Post's suggestion of treating cyberspace as a distinct space in and over which States have neither the legitimacy nor the power to rule.[32] Instead, private players, such as ISPs, online portals, domain-name registrars and other Internet-based law-making institutions, would rule within this independent cyber-jurisdiction.[33] This vision, bar very

[30] On the diversity of national criminal laws, see Bremer, above n. 7, 131ff, Goodmann and Brenner, above n. 7, 177ff.

[31] P. N. Grabosky and Russell G. Smith, *Crime in the Digital Age* (Leichardt, NSW: Federation Press, 1998), 10: 'It has taken decades to achieve a modest consensus about the merits of international mutual assistance in furtherance of combating drug trafficking and money laundering. Even in those nations characterised by agreement in principle, the actual implementation can be difficult ... Similar problems exist in relation to international copyright regulation and banking arrangements.'

[32] David R. Johnson and David Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367, although it is noteworthy that, even under their model of cyberspace law, the help of the State would be required, as it would be expected to enforce cyberspace law. The idea of 'netiquette' ranked high amongst the early Internet community and a revival of *lex mercatoria* was to close the gap left by the withdrawal of the State in the commercial context. Berman, above n. 7, 401ff. On self-regulation and its shortcomings, see Bremer, above n. 7, 66ff.

[33] Johnson and Post, above n. 32, 1378ff, 1383. For the purpose of this discussion, self-regulation is used in its frequently adopted very broad meaning encompassing everything from ordinary self-help measures to self-regulation through private institutions as well as self-regulation against a government framework. But it does not include measures taken by private actors, including ISPs in direct response to obligations imposed

few exceptions, has not been realised. States have, on the whole, not withdrawn as regulatory supervisors, perhaps mainly because it is simply impossible to separate the traditional sphere of State regulation from the online sphere. Not regulating cyberspace inevitably compromises and undermines traditional State regulation. For example, not recognising the possibility of online defamation would severely compromise the aim of general defamation law to protect individuals from unjustified slurs on their character. If States were not attempting to protect consumers from online rogue dealers or children from unsuitable online material, how effective would their overall protective role in respect of consumers or children be? Harmonisation through deregulation would stop States discharging their assumed and expected regulatory responsibilities. Like substantive harmonisation through treaties, harmonisation through deregulation would prevent States and their communities from holding onto their peculiar political, cultural and social values. Freedom of transnational online communications could be guaranteed, but at the expense of regulatory diversity. The market or private institutions would decide the regulatory bottom-line.

Nevertheless, some deregulation seems to have occurred. Certainly, States have strongly encouraged, and placed greater reliance on, self-help measures taken by end-users and intermediaries. But, importantly, traditional regulation has generally not been abandoned, but – given the difficulty of ensuring its efficacy due *inter alia* to States' impotence over foreign actors – private regulatory mechanisms have often had to come to the rescue. Spam is a case in point. In relation to the US legislation, it has been argued:

> the Act has been a total failure ... Less than 1 percent of unsolicited commercial email conforms to the Act's requirements ... The reasons for the failure of the Act lie not in flawed provisions introduced through industry lobbying, but in the structure of the Internet itself. Meanwhile private industry has made major strides in developing anti-spam measures.[34]

by national law, for example, under 'notice and takedown procedures', as this is considered 'ordinary' State law; cf. Ahlert, above n. 4, 125f.

[34] Peter B. Maggs, 'Abusive Advertising on the Internet (Spam) under United States Law' (2006) 54 *American Journal of Comparative Law* 385. 385. For a collection of privacy-protecting software, see Electronic Privacy Information Center, *Tools for Protecting Online Privacy*, www.epic.org/privacy/tools.html.

So more effective private measures not only supplement but indeed outshine traditional State regulation.[35] And there are many other examples of this type of self-help or private ordering. Online dispute resolution, as for example offered by eBay, supplements traditional dispute resolution through State courts, and these ADRs are not second-best, but for all intents and purposes often the only realistic, cost-effective solution in consumer disputes.[36] In the European Union, the Safer Internet Programme (1999–2004), followed by the Safer Internet Plus Programme (2005–2008),[37] is the express self-regulatory European response to illegal and harmful online content, including spam, that has proved ungovernable through traditional State regulation. The latter programme is introduced with the words: 'Illegal and harmful content and conduct has been a concern for lawmakers ... since the Web put [*sic*] unregulated content one click away from any Internet-connected PC. How illegal content is actually defined, depends on the country – what is illegal in one country can be protected as speech in another ... The problem ... cannot be tackled by legal measures alone.'[38] Self-regulatory measures promoted and set up by these programmes are hotlines allowing individuals to report illegal content,[39] the promotion of technological measures such as filtering used in combination with a rating system and quality labels as well as awareness-raising activities. For the purposes of this discussion, it is critical to realise that these self-regulatory

[35] Maggs, above n. 34, 389, where the author argues that the future lies in the adoption of an email authentication system coupled with an automatic rejection of non-authenticated emails.

[36] Again, this area has attracted a vast amount of research. OECD, *Legal Provisions Related to Business-To-Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection* (2002) DSTI/ICCP/REG/CP(2002)1/FINAL; American Bar Association (ABA), *Addressing Disputes in Electronic Commerce – Final Report and Recommendations of the American Bar Association's Task Force on Electronic Commerce and Alternative Dispute Resolution* (August 2002); Julia Hörnle, 'Online Dispute Resolution in Business to Consumer E-Commerce Transactions' (2002) (2) *Journal of Information, Law and Technology*, www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/hornle/.

[37] Decision No. 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a Multiannual Community Programme on Promoting Safer Use of the Internet and New Online Technologies (OJ L149/1, 2005) For more information, see http://europa.eu.int/information_society/industry/content/ or http://europa.eu.int/saferinternet/.

[38] European Commission, *Safer Internet Plus Programme*, Factsheet 18 (October 2005), http://ec.europa.eu/information_society/doc/factsheets/018-saferinternetplus.pdf.

[39] See, for example, Virtual Global Taskforce, www.virtualglobaltaskforce.com, a taskforce made up of police forces from around the world to fight online child abuse, to which reports of inappropriate or illegal online activity with respect to children can be reported, but currently only from the UK and Australia.

measures do not displace State regulation. There is no question of deregulation. These measures occur against the backdrop of State regulation and seek to remedy its weaknesses. European 'self-regulation' is not truly about bottom-up harmonisation, but about retaining State-centric regulation.[40]

One regulatory area to which States have indeed had little access is the coordination and allocation of the Internet's address system. It is the role of the Internet Corporation for Assigned Names and Numbers (ICANN), a Californian non-profit public-benefit corporation, 'to coordinate . . . the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems'.[41] While ICANN delegates control over country-code top-level domain registries,[42] and while its dispute resolution policy does not prevent trademark owners from bringing actions in State courts,[43] ultimate control over Internet addresses lies with ICANN and not with States, that is, except in the US.[44] This is not to say that States have had no influence over ICANN decisions. Indeed, some argue they have too much influence; others defend it as a necessary counterweight

[40] Despite plenty of rhetoric to the contrary, see e.g the European Commission, above n. 38, para. iv: 'There are many opinions on whether national rules should be harmonised – and how much. Issues include freedom of expression, proportionality and technical feasibility. The EU emphasises a self-regulatory approach, allowing different Codes of Conduct.' See also Council of Europe, *Declaration on Freedom of Communications on the Internet* (adopted by the Committee of Ministers on 28 May 2003), especially Principle 2: 'Member States should encourage self-regulation or co-regulation regarding content disseminated on the Internet.'

[41] Art. 1(1) of the Bylaws for ICANN, which also state that ICANN's role is to coordinate the allocation and assignment of domain names, IP and AS numbers and protocol and parameter numbers. On ICANN, see Feld, above n. 4; OECD, *OECD Input to the United Nations Working Group on Internet Governance (WGIG)* (2005) DSTI/ICCP(2005)4/FINAL, www.oecd.org/dataoecd/34/9/34727842.pdf, 23ff.

[42] Smith, above n. 7, 80; OECD, above n. 41, 23.

[43] ICANN's Uniform Dispute Resolution Policy (adopted in 1999 and implemented in January 2000) is designed to provide a 'fast-track' resolution process (in the case of bad faith registrations of gTLDs) but does not preclude judicial review.

[44] ICANN has a number of significant connections with the US: it is a company incorporated in the US, and headquartered in California and discharges functions previously carried out on behalf of the US government in particular by the Internet Assigned Numbers Authority (IANA). ICANN carries out its role pursuant to a contract with the US Department of Commerce, entered into in 1998, but signed a new Joint Project Agreement between the Department of Commerce and ICANN (29 September 2006), www.icann.org/general/JPA-29sep06.pdf, designed to move further towards the full management of the Internet's system of centrally coordinated identifiers through a multi-stakeholder model of consultation.

to US dominance.[45] But, at least officially, governments are just one of many stakeholders.[46] The relative independence of ICANN from States[47] can be explained partly by its historical origin and partly by the imperative of having a single ultimate controller of the Internet's address system for its proper functioning.[48] So this is not something States have had much choice about. ICANN's relative independence from States is also instructive as it highlights an almost invariable problem with regulation by private institutions: its democratic deficit and lack of accountability.[49] Although bottom-up harmonisation, or non-State regulation, is popularly perceived as more democratic, inclusive and libertarian, this is rarely the case – partly perhaps because the structures necessary to ensure and enforce accountability cannot easily be created outside the State paradigm.[50] But, be that as it may, for States such private-level 'harmonisation' certainly

[45] For example, ICANN, under pressure from the Australian government, transferred the .au ccTLD from Robert Elz (a friend of Jon Postel) to a non-profit organisation formed by the Australian government; discussed and criticised by Feld, above n. 4, 350, see also 355.

[46] Arts. XI and XI-A of the Bylaws for ICANN.

[47] But Feld, above n. 4, 335: 'ICANN's failure to persuade or coerce the DNS asset managers to enter into voluntary agreements forced ICANN to embrace a greater role for sovereign governments.'

[48] See above n. 44, and Feld, above n. 4, 333: 'ICANN represented a compromise between the Department of Commerce and various interest groups. Its primary purpose was not to privatize the management of the domain name system, but to centralize its control under the rubric of stability.'

[49] OECD, above n. 41, 23; Smith, above n. 7, 79ff; Elizabeth G. Thornburg, 'Going Private: Technology, Due Process, and Internet Dispute Resolution' (2000) 34 *UC Davis Law Review* 151, 192; Elizabeth G. Thornburg, 'Fast Cheap and Out of Control: Lessons from the ICANN Dispute Resolution Process' (2002) 6 *Journal of Small and Emerging Business Law* 191. Note, ICANN 's website (www.icann.org/general/accountability_review.html) states that ICANN is accountable to the 'community'. By Art. V of the Bylaws for ICANN, ICANN establishes the Office of the Ombudsman to evaluate and where possible resolve complaints about unfair or inappropriate treatment by ICANN. This seems a case of expecting the ombudsman to bite the hand that feeds it.

[50] See also Ahlert, above n. 4, 134f (on the lack of transparency of private technical standard-setting bodies, such as the Internet Engineering Task Force and the World Wide Web Consortium); Berman, above n. 7, 397ff (on the lack of procedural transparency and democratic legitimacy of bodies such as WIPO and WTO); Muchlinski, above n. 22, 230ff (on the lack of accountability by regulatory institutions such as TNCs and intergovernmental organisations). On the misleading rhetoric on the Internet's architecture, see Kathy Bowrey, *Law and Internet Cultures* (Cambridge: Cambridge University Press, 2005), 8: 'the culture that has grown up around the internet uses references to the voluntariness of the "protocols" the virtues of "decentralisation" and "openness" and the "choice" about compliance ... This language, used especially by those technicians and managers whose actions power the system, deflects any address toward the reality of decision-making structures existing.'

comes at a price: ultimate control over matters affecting their territory is in the hands of an outsider.

In summary, substantive legal harmonisation by design has been the preserve of a few very specific legal areas where States had either no choice or a strong common interest or concern in respect of the regulatory activity. Substantive harmonisation remains rare because it is not as flawless a solution as is often made out. While it would be in tune with the borderless Internet (i.e. facilitate both uninhibited global communications and more efficient regulation), harmonisation by definition rejects legal diversity. However, there is a reality of vast cultural, social and political diversities amongst States and that reality is mirrored by, and reinforced through, legal differences across the regulatory board.[51] Although the idea of protecting national legal values against and in cyberspace may appear anachronistic, paternalistic and anti-libertarian, the alternative is often perceived as worse. Harmonisation by treaty entails a negotiated compromise; and that compromise is by definition a 'loss' to the participating States and only justifiable by the good flowing from the overall consensus. Given the unequal bargaining powers between States, the weight of that compromise tends to be felt by the weaker States.[52] In any event, that 'loss' would be magnified in the online context, as harmonisation would have drastic repercussions for large chunks of the domestic law – given both the regulatory ambit of online activity and the fact that it is often not realistic to separate equivalent online and offline activity.[53] Not surprisingly, States have generally resisted a global solution to online activity.

C. Substantive harmonisation by default

Global legal standards sometimes occur by design, but more often than not in the online world they occur by default or *de facto*. Harmonisation

[51] Particularly in respect of certain types of activity, see above n. 25.

[52] On the political reality of international-law-making, see Michael Byers, *Custom, Power and the Power of Rules* (Cambridge: Cambridge University Press, 1999), Chapter 3. On the US dominance in negotiations on global IP standards, see e.g. Bowrey, above n. 50, 188ff. Note, too, the effectiveness of substantive harmonisation would be seriously undermined even if only a few States failed to participate as these States could become online content havens.

[53] In other words, in respect of most legal areas affected by the Internet, the regulation is technology-neutral, that is, not Internet-specific; anti-spam regulation is a notable exception. In other legal contexts, for example the high seas or outer space, the harmonised area can be separated more easily from the domestic legal sphere of the State.

by default can occur in two different ways; they have in common that, while States ostensibly hold onto their diverse national laws, they do so more or less unsuccessfully. When one enters different States in the real world, their distinct laws become readily apparent in a myriad of ways. For example, in Amsterdam the open availability of cannabis in coffee shops suggests its legality in the Netherlands. From the fact that British pubs are often home to gambling automats, one can safely deduce that these are legal in Britain. As youngsters can often be seen on mopeds in France, the permissible driving age for mopeds may be assumed to be lower in France than in the UK or Germany. Such apparent differences in the availability of goods or in common activities are not always based on different laws; it could be that teenagers in the UK or Germany do not consider mopeds cool, or that cannabis simply enjoys no popularity outside the Netherlands. So if in the real world something is *not* readily available, this omission tends to be inconclusive as to its illegality; however, if something *is* openly available or regularly done, this tends to suggest quite conclusively its legality.[54] This real-world phenomenon of law being reflected in behaviour holds much less true in cyberspace. Regardless of the location from which one enters cyberspace, much of the material is the same. Whether one enters cyberspace from the US, France or Germany, Nazi memorabilia can be accessed from all three locations – even though it is legal only in the US. Whether one checks one's email from Germany, Australia or the US, spam is always present, even though unsolicited commercial email is banned in Germany and Australia, and is controlled in the US. Actual online activity is not (or only marginally) in tune with the respective national legal requirements; it is a relatively uniform activity regardless of one's location. Although the law is not actually harmonised, in reality it is so ineffectively enforced and routinely breached that it is as if it were non-existent. But let us briefly examine how this *de facto* or default harmonisation fits into the general jurisdictional debate.

The country-of-destination approach

As seen from previous chapters, in relation to most regulatory concerns, public or private, States have adopted a country-of-destination approach to the competence issue, and this is again the case in respect of spam. For example, the Australian Spam Act 2003 (Cth) prohibits

[54] There are exceptions where a law is routinely broken e.g. speeding or drink-driving.

unsolicited commercial electronic messages with an Australian link.[55] That link is established, either if the message originated or was commissioned in Australia or, critically here, originated outside Australia but was accessed in Australia.[56] Similarly, the US Controlling the Assault of Non-Solicited Pornography and Marketing Act (2003), known as the CAN-SPAM Act, is also applicable to commercial emails originating from outside the US. The restrictive provisions are directed to electronic messages sent to a 'protected computer',[57] which is defined as any computer 'used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States'.[58] The focus is on the location of the effect of the message; indeed, the US even purports to regulate messages sent *and* received outside the US, if those messages have an effect on US domestic or foreign commerce. Unlike in Australia, unsolicited electronic messages are not prohibited *per se*, but must provide the customers with an opportunity to opt out of receiving future messages.[59] The US adopts an opt-out approach rather than the opt-in approach favoured in Australia and the EU. The relative merits of either approach are of no further interest here: what is of interest is how these two distinct national approaches fit within the transnational Internet.

Assuming that each State can enforce its provisions over local spammers, there are effectively two scenarios with respect to foreign spammers. First, there is the respectable foreign spammer or, less pejoratively, commercial advertiser.[60] He could try to make his commercial emails directed at Australian residents compliant with Australian law, and the same with regard to the US; that is, he could try to segregate territorially his online activity (discussed further below). The equivalent measure with websites would be to have country-specific websites disallowing access from outside the targeted State. The main problem the online

[55] Section 16 of the Spam Act 2003 (Cth).

[56] Section 7 of the Spam Act 2003 (Cth). Under this section, an Australian link appears to exist in respect of messages accessed in Australia by, for example, a tourist from the UK with an UK-domain email address. Conversely, no link exists if an Australian with an Australian email address accesses it in the UK.

[57] See s.5(a)(1), (3)(A), (4)(A) and (5) of the CAN-SPAM Act (2003) (alternatively, see 15 United States Code Annotated §7704).

[58] 18 United States Code §1030(e)(2)(b).

[59] Section 5a(4)(A) of the CAN-SPAM Act (2003).

[60] This includes many highly respectable online businesses with an interest in the online marketing of their products.

advertiser faces with that option is determining with which physical location his email addresses are connected.[61] Often, email addresses have no obvious or necessary correlation with any State; absent actual contacts with the respective customers, locating them is a guessing game and even then not entirely reliable. Geo-location tools may determine reasonably accurately from where an actual email came, but cannot predict where that person may access his emails in the future.[62]

Given the difficulty of territorially segregating email messages, the safest and *only* other option for the respectable advertiser[63] is 'personally' to harmonise Australian and US (and indeed all other anti-spam laws) by complying with the strictest one, in this case the Australian prohibition on unsolicited email. Just ascertaining the strictest legal standard would generally be an extremely onerous exercise given the number of States involved. Yahoo! Inc. personally harmonised laws on hate speech when it decided to change its policy to disallow neo-Fascist material, consistent with the French prohibition but not inconsistent with the more permissive US free-speech standard.[64] *De facto* substantive harmonisation occurs as the online actor seeks to comply with all legal standards by complying with the strictest one or the highest common denominator. By implication, he loses the benefit of the lower legal standards of most other States, and those States lose the benefit of his online speech and activity that they would permit but another State does not. Legal diversity is lost. The main advantage gained by the advertiser is that he need not territorially differentiate between his customers, and thus uninhibited transnational online communications is gained. But to what avail? – the permissible content of such communications is severely restricted.

While this type of *de facto* harmonisation has often been used to show the alarming consequences of adopting a country-of-destination

[61] Under Australian law, above n. 56, whether the email is accessed in Australia regardless of its domain name; under US law, above n. 58, even if an email is accessed outside the US, if the recipient is a US resident, it still has a connection with US domestic or foreign trade.

[62] Svantesson (2004), above n. 1, 109ff, where the author explains that current geo-location technology simply translates IP addresses into geographic locations. Website operators are in a better position as surfers, by accessing a site, reveal with the help of geo-location technology their own location.

[63] Discounting other alternatives e.g. looking for another job or becoming a rogue spammer.

[64] See *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199 (9th Cir. 2006), discussed in depth in Chapter 6.

approach to competence, it has not been borne out by reality. It is not the respectable spammer who is the problem, but the rogue spammer or, more worryingly, the common advertiser.[65] Two factors determine their behaviour and provide them with strong incentives to ignore relevant foreign legal expectations: first, trying to comply with all those foreign laws presents an overwhelming regulatory burden; secondly, not complying with them presents few risks given States' general inability to enforce their laws abroad. At best, these spammers comply with the law of the State in which they are established; again, they 'personally' harmonise the laws of all the States theoretically applicable to their activities by complying only with local law. While this self-adopted origin rule seems to allow for regulatory diversity given that spammers have different origins, it certainly creates an incentive to move advertising operations to the State with the lowest legal standard. In any event, *de facto* harmonisation occurs not just for the spammer deciding to comply only with local law, but also for States as they lose the benefit of their stricter laws through the infiltration of foreign illegal spam. The *de facto* regulatory bottom-line is set by the spam from the least regulated State. As the legal hurdles for transnational online activity are disregarded, transnational communications are uninhibited[66] and national legal diversity is again lost, *de facto*.

Last but not least, does a moderate country-of-destination approach – in the form of a directing or targeting analysis – change the dynamics of the irreconcilability argument? Fundamentally not. A targeting approach is comparable to trying to reconcile the size 14 person with a size 8 jacket by making the jacket a bit larger and the person a bit slimmer, so that they meet somewhere in the middle. In other words, a targeting approach (assuming the regulatory claims of targeted States can be enforced) both inhibits transnational communications and undermines national legal spaces, but in both cases only moderately so. According to the targeting approach, States have a right to regulate a foreign online content provider only if they were the specific target of his activities. All States mildly affected by his foreign activity, but not specifically targeted, must tolerate it and thus tolerate their distinct national laws being

[65] The relative percentage of rogue actors within the industry is likely to vary from industry to industry and would appear to be higher in the context of spam. See Raw, above n. 8, 39: 'It is thought that less than 200 spammer companies are responsible for 90% of junk email.'

[66] Such a hurdle in the case of respectable spammers is the self-imposed idea that foreign laws ought to be complied with.

slightly undermined. By the same token, an online content provider's freedom to communicate freely with foreigners without being exposed to the laws of their States is very restricted: it only applies to isolated and occasional contacts. Once he goes beyond that, he will be taken to have targeted the State and will face exactly the same options as those outlined above in respect of spammers: either territorially segregate his activities or 'personally' harmonise the varying legal standards at the highest or lowest (or local) legal standard – each having clear costs and benefits. Finally, it must be remembered that States suffer the same enforcement problems whether they adopt an outright or a moderate destination approach to competence, that is, whenever they seek to apply their laws to foreigners on the basis of the local effects of the foreign activity. And this impotence by States encourages foreign national law not to be taken seriously and thus *de facto* harmonisation at the lowest regulatory standard.

The country-of-origin approach

Is the exclusive country-of-origin approach to competence, as discussed in Chapter 5, in any way more successful in truly reconciling the transnational Internet with national law? On the face of it, it seems to retain regulatory diversity while at the same time not expecting online actors to comply with the laws of all the foreign States with which they come into contact in the course of their online activity, thus facilitating unrestricted global communications. But is this indeed the case?

The EU has responded to spam with a regionally harmonised response. Article 13(1) of the Directive on Privacy and Electronic Communications[67] goes substantively along the lines of the Australian opt-in approach by prohibiting *unsolicited* commercial email: 'The use of . . . electronic mail for the purpose of direct marketing may only be allowed in respect of subscribers who have given their prior consent.' But, in contrast to the US and Australia, the EU adopts an exclusive country-of-origin approach to spam regulation; it does not extend its restrictive provisions to non-EU spammers.[68] This approach is

[67] Directive on Privacy and Electronic Communications, 2002/58/EC, implemented in the UK by the Privacy and Electronic Communications (EC Directive) Regulations 2003, see reg. 22; UK Department of Trade and Industry, *Implementation of the Directive on Privacy and Electronic Communications* (March 2003), www.dti.gov.uk/files/file15097.pdf.

[68] *Ibid*., 15: 'Calls from overseas marketers have started to generate complaints; the Directive does not apply outside the EU.'

consistent with the one taken in the Data Protection Directive which only applies to data controllers who are either established within the EU or use equipment within the EU to process data.[69] The question is how this origin approach fits into the general argument of this chapter about the irreconcilability of national law and the transnational Internet.

First, within the purely EU spamming context, the origin rule operates against the background of substantive regional harmonisation, as provided for by the Directive. The origin rule is not really there to choose between different State laws to determine which one is to be applied to which spammer (given that all the laws are substantially the same), but rather to allocate which State has the responsibility (and not simply the right) to ensure compliance with the EU-wide legal standard.[70] In other words, the point of the competence rule is not to preserve legal diversity but quite the opposite: to guarantee the harmonised standard by allocating who has to administer it when.[71] And these harmonised standards come with all the advantages of harmonisation, i.e. uninhibited communication as well as effective law enforcement – but only within the harmonised region, which brings us to the second scenario.[72]

Vis-à-vis the rest of the world, any harmonised region is effectively in the same position as an individual State normally is; in the online regulatory context it creates a conflict between regional (rather than national) law and the global Internet. Within the wider global context,

[69] Art. 4 of the Data Protection Directive, 95/46/EC. To protect the privacy of individuals within the harmonised region effectively, the Data Protection Directive, 95/46/EC, extends its provisions to transfers of personal data to States outside the EEA, and allows such transfers only if the third State has 'adequate levels of [privacy] protection'. See, for example, Safe Harbour Principles applicable to the US. Online website operators in control of personal data need to restrict access to their sites from the 'inadequate' States. Smith, above n. 7, 372f. However, the European Court of Justice took a moderate approach in *Bodil Lindqvist*, Case C-101/01 [2004] 1 CMLR 20, when it decided that the publication of personal data on a private website dedicated to the activities of a Swedish church did not amount to a 'transfer of data to a third country' under the Data Protection Directive even if such data was thereby made accessible to persons in third countries.

[70] Although different Member States may be more or less vigilant in pursuing wrongdoers, the application of the origin rule generally presupposes a certain mutual trust in the foreign legal systems.

[71] See the discussion Chapter 5, section 2.B, above (Electronic Commerce Directive).

[72] This is again a case of a halfway house, i.e. national law and the transnational law moving towards each other: the globalisation of law stops at the EU borders and thereby creates the need to guard uninhibited online communication coming from, and going beyond, these EU borders.

the EU origin rule in respect of spamming again does not preserve legal diversity – albeit for different reasons than in the pure EU context. The origin rule means that foreign spam is simply not subjected to local law. This hands-off attitude to non-compliant foreign spam is highly problematic if, as must be assumed, the aim of the regulation is to reduce substantially the amount of spam. But, in terms of actual consequences, an origin approach is hardly distinguishable from an ineffective destination rule (which, as discussed above, often leads to a self-adopted origin rule by the spammer).[73] In both cases, the *de facto* legal standard is again set by the lowest common denominator worldwide.

Not surprisingly, spam has remained a problem in all the examples chosen in the above discussion, in Australia, the US and the EU, quite regardless of their different substantive laws and jurisdictional stances. The International Telecommunication Union comments on a study on spam in Belgium: 'Amongst the more interesting findings was the fact that the majority of the emails were being sent from outside Belgium – in particular the US.'[74] In Australia, 'less than two per cent of spam received by Australians [is] now coming from Australian sources'.[75] Even the US suffers similarly: 'only 1 percent of spam e-mails ... complied with CAN-SPAM ... The problem with the CAN-SPAM law is that of the 1 million spam messages ... tracked ..., 40 percent came from outside the US, spread across IP (Internet Protocol) addresses in 152 nations.'[76] Larger, more economically powerful States, such as the US, invariably have a higher percentage of home-grown to foreign content and are thus slightly advantaged in terms of controlling online activity. Nevertheless, the reality of *de facto* legal harmonisation is, at least in all Western democratic States, undeniable and explains the popular perception that the Internet is unregulated. And yet, despite the reality of rock-bottom online legal standards, States still resist harmonisation by design or, alternatively, cooperation in creating national online cyberspaces, and to this latter matter the discussion turns now.

[73] Unlike the destination rule, the origin rule almost overtly encourages forum-shopping and thereby a regulatory race to the bottom; see the discussion in Chapter 5, section 2.B, above.

[74] ITU, above n. 9, 14.

[75] Australian Communications and Media Authority, 'ACA Signs London Action Plan on Spam', Media Release No. 6 (22 February 2005).

[76] Grant Gross, 'US Anti-Spam Law Still Not Making a Difference' (2 April 2004), Techworld, www.techworld.com/security/news/index.cfm?newsid=1332/.

3. A less transnational Internet

The only alternative to harmonisation or more global law, either by design or default, is a less global Internet, that is, restricted transnational communication, more clearly demarcated national cyberspaces. And, despite much liberal rhetoric to the contrary, the online and offline preservation of their peculiar national legal standards is what most, if not all, States including Western democratic States aspire to, and not infrequently quite aggressively so. The idea of a less transnational Internet is generally met with scepticism. Yet it occurs already in a variety of ways, often with the help of technological measures. These technological measures are being used by both private players and public players, to further both self-regulation and traditional State regulation. Technology, or in Lessig's terminology 'code',[77] has no *prima facie* regulatory loyalties. Furthermore, technological and other measures to limit the territorial reach of online activity may be employed either in the country of origin of online activity or in the country of receipt or destination of that activity. While these measures differ in their effectiveness, transparency and invasiveness, they all have the effect of territorially zoning online activity and recreate traditional State boundaries in cyberspace.

A. Zoning in the country of origin

The most effective and fair way of tackling any illegal activity is at its source, at the location where the wrongdoer is established: the country of origin. This may be done either by inducing the foreign wrongdoer 'voluntarily' to avoid illegalities on foreign shores, or by relying on the cooperation of his State of origin to induce compliance or take restrictive actions itself. Generally, zoning in the country of origin assumes, and is done in response to, extraterritorial regulatory claims by foreign States (competence asserted over activity on the basis of a country-of-destination approach).

As to State cooperation, which has been explored in Chapters 5 and 6, suffice to say that generally States' willingness to cooperate in the enforcement of each other's law is very limited in respect of their private laws and non-existent in the public-law sphere. Lessig's proposal, however well intentioned, of reciprocal enforcement whereby '[e]ach state

[77] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

would promise to enforce on servers within its jurisdiction the regulations of other states ... in exchange for having its own regulations enforced in other jurisdictions'[78] has not had much uptake,[79] and for reasons explained in Chapter 6[80] is unlikely to have any more in the near-to-medium-term future. Nevertheless, the principled willingness of States to enforce each other's private laws goes towards compelling online actors to respect foreign private law, which brings us to the 'voluntary' territorial zoning option available to online content providers.

Regardless of the actual ability of States to enforce their laws against foreign actors, respectable high-profile online actors and businesses do not want to be seen to flout foreign laws.[81] Apart from 'personally' harmonising all foreign law applicable to their online activities at home and abroad, the only other option is to territorially 'split' their online activities to be responsive to the different national legal requirements. This can be done in two ways. First, online content providers can create different sites for different territories, as large Internet businesses, such as Yahoo, eBay, Google, Amazon and Expedia, do and make these sites responsive to the varying local legal requirements.[82] Google has removed neo-Fascist material from its German and French News index, and in respect of its Chinese site it removed links to news sources the Chinese government had blocked.[83] The option of concurrent sites is attractive for large commercial players as there are also generally sound commercial reasons to have differentiated sites to take account of different languages and cultures. However, having these dedicated sites does not always by itself protect companies from being exposed to the laws of States other than the specific State targeted by the site – certainly

[78] *Ibid*., 55f.

[79] For notable exceptions, see the UK and Australian online gambling legislation, discussed in Chapter 5, section 3.B, above.

[80] Chapter 6, section 3.B and 4.C, above.

[81] Chapter 6, section 2.B.

[82] Contrast, for example, the choice-of-law and choice-of-forum clauses on expedia.com (www.expedia.com/daily/service/legal.asp) and expedia.co.uk (www.expedia.co.uk/daily/service/legal.asp?CCheck=1&/). Compare also Conditions of Use for the US and UK Amazon site. In these cases, the companies often 'go' to the country of destination with subsidiaries and upload the site onto servers there.

[83] Note, this was in respect of a site which was hosted from outside China. Google has since hosted its site from servers within China and complied with various censorship requirements by the Chinese government; see Danny Sullivan, 'Google Now Censoring China' (25 January 2006), SearchEngineWatch, http://blog.searchenginewatch.com/blog/060125-072617/; Susan Kuchinskas, 'Google Axes Hate News' (23 March 2005), Internetnews.com, www.internetnews.com/xSP/article.php/3492361/.

not in the public law context where the targeting approach has never been adopted. The yahoo.com site did not escape French law either by virtue of it being directed mainly at the US or by virtue of the existence of the dedicated yahoo.fr site.[84] For these sites to insulate themselves against foreign law they would have to exclude users from all but the targeted State, that is, not just territorially *zone* their sites, but territorially *seal* them.[85]

This brings us to the second zoning option which is simply the exclusion of all foreign customers (without any concurrent country-specific sites) – an option more feasible for smaller players for whom country-specific, legally tailored websites would be unrealistic, or even for large players whenever the profits to be gained from a State would be comparatively small. Svantesson refers to ShowTime and its site www.sho.com which – when accessed from outside the US – displays the message: 'Sorry. We at Showtime Online express our apologies; however, these pages are intended for access only from within the United States.'[86] To avoid this very scenario some objected to the destination rule in EU consumer contracts: 'a "country of destination" principle would divide the Single Market into fifteen different markets because retailers, fearing the risk of litigation in foreign states, might offer their products only to consumers domiciled in the same State as the one in which the retailer is established.'[87] Applied to the spamming context, this zoning option means that the marketer tries to ensure that

[84] Currently, very few sites seem to deny access on the basis of location even where concurrent sites exists. *Yahoo! Inc.* v. *LICRA and UEJF*, 433 F 3d 1199, 1202 (9th Cir. 2006): 'In actual practice, however, national boundaries are highly permeable . . . [A]ny user in the United States can type www.fr.yahoo.com into her web browser and thereby reach Yahoo! France's website.'

[85] For some legal purposes it may be sufficient to reject actual transactions with consumers from certain States; for other purposes access to the site would have to be denied to avoid legal exposure; see e.g. *R* v. *Perrin* [2002] EWCA Crim 747, where allowing access to the site gave rise to the obscenity offence. Similarly, for defamation purposes or under German or French hate speech law, the simple viewing of the offending material would be sufficient to attract liability.

[86] Svantesson (2004), above n. 1, 110f. See also Joel Reidenberg, 'Technology and Internet Jurisdiction' (2005) 153 *University of Pennsylvania Law Review* 1951, 1961: 'RealNetworks, for instance, only streams soccer games to users in particular countries.'

[87] Joakim S. T. Oren, 'International Jurisdiction over Consumer Contracts in e-Europe' (2003) 52 *International and Comparative Law Quarterly* 665, 671; and he continues at *ibid*., 672: 'However, the same scenario was put forward by the consumer organisations, as they predicted that a "country of origin" principle would deter consumers from buying product from foreign retailers, if they were not allowed to seek remedies in relation to potential disputes in the courts of their own state of domicile.'

his messages only reach customers in his home State. Although this second zoning option is a variation of the first, it is more troublesome. It is more realistic for the vast majority of online providers, and under it online providers exercise drastic self-censorship – at a substantial cost to the online community. They restrict access to their content or products not because it *is* illegal, but because it *may* be *illegal or may* give rise to foreign litigation. Often, this may not in fact be the case, but the burden of ascertaining the foreign law or the risk of foreign litigation is simply too great. However, the very fact that the business opts for screening suggests that it is a prudent, generally law-abiding business.

Territorially sealing sites presupposes that content providers are able to identify the location of those accessing their site (or those receiving the commercial email) and this is where geo-location technology comes into play. Today, there is a range of increasingly sophisticated and affordable software tools that allow providers to recognise the location of surfers who access their sites and exclude them if need be.[88] While technologically adept users can circumvent these measures, the majority of ordinary users cannot. And, depending on how such exclusions are presented to the user, they may not even realise that a deliberate exclusion has occurred.[89] Currently though, most sites by well-known operators do not exclude foreigners, as Show Time does, but gently redirect them. Expedia and Amazon redirect those who choose the 'wrong' site to the 'right' corresponding country-specific site. 'Google's geolocattion

[88] Svantesson (2004), above n. 1, 109f: these tools match IP addresses to physical location, and their accuracy varies depending on the context. The author also refers (*ibid.*,120f) to less sophisticated methods which, if bundled, may also yield fairly reliable results, e.g. relying on the language, time zone, and the location setting of the user's language. For one opinion on the likely future of geo-location technologies, see Benjamin Edelman, 'Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users' (Expert Memorandum attached to the National Association of Broadcasters' submission to Industry Canada) (2001), http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf; Saskia Sassen, 'The Impact of the Internet on Sovereignty: Unfounded and Real Worries', in Christoph Engel and Kenneth H. Keller (eds.), *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values* (Baden-Baden, 2000), 196, www.mpp-rdg.mpg.de/pdf_dat/sassen.pdf, where the author argues that '[w]e cannot take its "seamlessness" as a given simply because of its technical properties'.

[89] On circumvention methods, see Svantesson (2004), above n. 1, 113f. Circumvention efforts presuppose an awareness of the intentional exclusion, which may not always be the case: Ahlert, above n. 4, 131, mentioning as an example AOL's decision to block emails from Oxford University's email system to AOL email addresses. The blocking was done in a way which suggested to the user that there had been a technical problem, when the email was returned to the sender.

systems typically automatically offer . . . sites to users in the corresponding countries.'[90] But users tend to retain the option of accessing site not corresponding to their country of residence.

At times actually acquiring goods or services is made dependent on residence. For example, the 'Terms of Use' of some websites, most notably those offering pharmaceutical goods and financial services, contain a term along the following lines: although it is accessible worldwide, this website and its content are intended only for residents of the United Kingdom.[91] Yet again, the wording of such Terms and Conditions often does not categorically preclude transactions with foreigners, and seems deliberately ambiguous. For example, the website of the large pharmaceutical company Pfizer states:

> Void Where Prohibited. This website and its contents are intended to comply with the laws and regulations in the US. Although the information on this website is accessible to users outside of the US, the information pertaining to Pfizer products is intended for use only by residents of the US. Other countries may have laws, regulatory requirements and medical practices that differ from those in the US. This site links to other sites produced by Pfizer's various operating divisions and subsidiaries, some of which are outside the US. Those sites may have information that is appropriate only to that particular originating country. Pfizer *reserves the right* to limit provision of its products or services to any person, geographic region or jurisdiction and/or to limit the quantities or any products or services we provide. Any offer for any product or service made on this website is void where prohibited.[92]

Pfizer does not categorically preclude transnational transactions; it discourages them, or wants to be seen to do so – not unlike Expedia's or Google's policy of 'gently' redirecting users.

[90] Jonathan Zittrain and Benjamin Edelman, 'Documentation of Internet Filtering Worldwide', in OSCE (Christiane Hardy and Christian Möller), *Spreading the Word on the Internet* (Vienna: OSCE, 2003), 137, 139.

[91] For example, Par Pharmaceuticals, www.parpharm.com/term.jsp; or ICOS, www.parpharm.com/term.jsp. See also Marks & Spencer's Terms and Conditions: 'Use of this website from outside the UK: Unless otherwise specified, the materials on this website are directed solely at the those who access this website from the United Kingdom. Marks & Spencer make no representation that any products or services referred to in the materials on this website are appropriate for use, or available, in other locations. Those who choose to access this site from other locations are responsible for compliance with local laws if and to the extent local laws are applicable.'

[92] Pfizer, www.pfizer.com/pfizer/mn_terms.jsp (emphasis added).

Given the many decisions discussed in previous chapters, where courts have explicitly endorsed the need for exclusionary measures,[93] it is surprising that so few sites are territorially sealed either at the accessing or at the buying stage, and categorically so. Mere lip-service to zoning does not appease foreign States,[94] and the safest legal route by far is the ShowTime approach: a national website externally sealed. What would be lost though is the transnationality of online communications, the benefits of which most online actors and most States are not willing to forego. In purely economic terms, a local commercial site restricted to the domestic sphere writes off all the potential rewards from foreign online markets.

As territorial zoning by online content providers and marketers cannot be compelled by the country of destination and has generally not been compelled by the country of origin (the latter having too much to lose), it has been rather half-hearted. In terms of motivation, it ranks at the same level as 'personal' harmonisation at the highest common legal denominator; both are forms of legal compliance exercised at significant cost in the absence of any real coercive threat. By far the preferred option for online content providers has been non-compliance with foreign law, or 'personal' harmonisation at the lower end of the legal spectrum.

B. Zoning in the country of destination

If illegal content is not restrained at its source, it has to be dealt with where it takes effect. Chapter 6 already discussed the various unilateral enforcement mechanisms available to States within their own territories and need not be repeated here.[95] The main point here is that, if content providers cannot be persuaded to territorially seal their sites (i.e. stop them from being accessed by foreigners), States can try to territorially seal their borders against the foreign online invaders, and thereby protect their

[93] Chapter 4, section 3.D, above. The most high-profile one being the Yahoo case: *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000), affirmed in *LICRA and UEJF* v. *Yahoo! Inc. and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000), www.foruminternet.org/actualites/lire.phtml?id=273/.

[94] As noted in previous chapters, private contractual clauses, disclaimers and easily circumvented exclusions cannot protect an online actor from exposure to the law of a foreign State, particularly when there are actual contacts with its residents. See also Svantesson (2004), above n. 1, 123ff. See Chapter 4, nn. 160–4, and the accompanying text.

[95] Chapter 6, section 3.C, above.

distinct national laws and legal standards. Again, such territorial zoning may be implemented either by private parties or by the State itself.

As companies have the option of drawing territorial boundaries around their sites (as their only alternative to 'personal' legal harmonisation), so have consumers the option of drawing boundaries around local sites, shunning foreign ones out of fear of legal uncertainties.[96] Also, rather than accepting the lowest common content denominator, many parents use filtering or blocking tools to protect their children against harmful and illegal content.[97] Junk filters and other software help to guard against spam, and anti-spy and anti-virus programs protect against malicious incoming software.[98] None of these programs are specifically directed at illegal foreign content. Yet, in so far as States are successful in dealing with local offenders (as, for example, the Australian and Belgium spam situations show[99]), these software tools fill the gap in respect of the foreign threats against which States are helpless. Effectively, in these cases it is left to the end-user to seal himself against illegal *foreign* content.

When such 'private' redrawing of national legal boundaries has been considered unreliable or inadequate, which no doubt it frequently is,[100] States themselves may try to seal their borders and block illegal content. This has generally found more favour in authoritarian regimes, principally because they are less concerned about the 'collateral' damage caused by the aggressive blocking measures (i.e. overblocking) in terms of both civil liberties and lost economic opportunities.[101] One commentator noted:

[96] This applies quite regardless of whether the consumer's jurisdiction applies a country-of-origin or country-of-destination approach, as the foreign business will often not comply with the law of the consumer's State in any event.

[97] For the usage of blocking and filtering tools in the twenty-five EU States, see European Commission, *Special Eurobarometer 250 'Safer Internet' Report* (May 2006), http://europa.eu.int/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf, 26f.

[98] Reidenberg, above n. 86, 1961f: 'Verizon . . . refuses to accept all email originating in Europe in an effort to combat spam.'

[99] See above nn. 74 and 75 and the accompanying text.

[100] See European Commission, above n. 97, 26f: although in the EU many parents use blocking software, a relatively high proportion of children still comes across illegal or harmful content.

[101] The risk of overblocking, that is, the 'accidental' blocking of legal and valuable content, is a concern in respect of all blocking initiatives: see e.g., in the context of spamming, Bowrey, above n. 52, 6f; see also Shanti Kalathil and Taylor C. Boas, 'The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution'

> at least 20 countries significantly restrict Internet access; many of them are engaged in cat-and-mouse struggles over web-access ... Thus, Singapore and the United Arab Emirates force all Internet traffic through a single gateway. The Singapore Broadcasting Authority since 1996 has regulated access to content by licensing both domestic websites and ISPs. The ISPs must install a 'proxy server' which will filter out content deemed objectionable by the government. The service providers are required to block access to sites that the government considers to undermine public security, racial and religious harmony or public morals.[102]

This type of zoning has been criticised as illegitimate government censorship.[103] A marginally more subtle form of government censorship is to 'persuade' local providers to exercise self-censorship. So, in return for being able to base its servers in China and provide faster access, Google has agreed to remove content from search results on google.cn not in tune with Chinese law and policy.[104] Such indirect censorship seems equally illegitimate until one considers that, in a different legal context it is also exercised by a democratic State.[105] Take, for example, US government pressure on local credit institutions to disallow transactions by local punters with foreign online gambling enterprises, or New

(2001) Carnegie Endowment Working Papers, Global Policy Program No. 21, www.carnegieendowment.org/files/21KalathilBoas.pdf; Kristina M. Reed, 'From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce' (2000) 13 *Transnational Lawyer* 451. On overblocking, see also Benjamin Edelman, *Empirical Analysis of Google SafeSearch* (2003) and *Web Sites Sharing IP Addresses: Prevalence and Significance* (2003), Berkman Center for Internet and Society, http://cyber.law.harvard.edu/home/. See also above n. 98.

[102] Denis T. Rice, '2001: A Cyberspace Odyssey Through US and EU Internet Jurisdiction Over E-Commerce' (2001) 661 *PLI/Pat* 421, 453. See also Zittrain and Edelman, above n. 90, 143: 'In certain countries, Internet connections are designed in a way that passes all communications through central facilities, directly facilitating centralized filtering. For example Saudi Arabia has designed its network in precisely this way.'

[103] Smith, above n. 7, 530: 'Another possible response ... is the retrograde, and technically difficult, solution of governments or other national authorities seeking to impose technical methods of blocking content at their virtual borders (i.e. their domestic ISPs).' On the effectiveness of blocking measures, see Goodman and Brenner, above n. 7, 213; Svantesson (2006), above n. 1, Part 3.4; Kalathil and Boas, above n. 101. 10ff. Online Policy Group Inc, *Why Blocking Technology Can't Work*, www.onlinepolicy.org/research/blockcantwork.shtml.

[104] Sullivan, above n. 83; see also Bowrey, above n. 50, 196.

[105] In this context, it is easy to confuse a disapproval of blocking with the substantive law protected through blocking. The difference between blocking by authoritarian regimes and democratic States lies in the detail: to what extent clear illegality has to be proven before such enforcement measures can be justified. Reidenberg, above n. 86, 1964f. See Smith, above n. 7, 529, on the EU attitude to blocking.

Zealand's prohibition on advertising or otherwise facilitating gambling with foreign online providers.[106] This, too, is governmental censorship. Democratic States may not censor political speech,[107] but they feel quite unconstrained in respect of economic speech or speech that is contrary to their moral or cultural values: 'Some states worry about attacks on their cultural identity, while others are more apprehensive about loss of control over their economic future.'[108] In the EU, the outright commitment against censorship and blocking by public authorities in the Draft Declaration on Freedom of Communication on the Internet became rather more qualified in its final version: 'measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.'[109] Again, increasingly sophisticated technological tools help States to implement such blocking measures, and again such measures can be circumvented by sophisticated users, but are for most intents and purposes effective in denying access to illegal foreign content.[110]

The main point here is not to give an exhaustive list of blocking measures available to States or private individuals to exclude illegal foreign content, but rather to show how borders may be, and have been, redrawn in cyberspace at the point of receipt. These borders are of varying security and transparency, but they all aim to guard the national legal space. That itself is hardly objectionable, even if one objects to the substantive legal standards protected by some States. Certainly, the point here is not to condemn censorship and the blocking of foreign content *per se*; much of traditional regulation impacts on communications and is restrictive and thus censors 'speech', as, for example, laws on misleading advertising, defamation law or licensing

[106] Chapter 5, section 2.A, above. Zittrain and Edelman, above n. 90, 144: 'In 2002, the state of Pennsylvania passed a law that requires ISPs to filter designated websites found to have distributed child pornography' (internal marks omitted).

[107] With some notable exceptions, such as the regulation of hate speech in Germany and France or, more recently, speech encouraging terrorism.

[108] Pierre Trudel, 'Jurisdiction over the Internet: A Canadian Perspective' (1998) 32 *The International Lawyer* 1027, 1027.

[109] Principle 3 of the Declaration on Freedom of Communication on the Internet (adopted by the Committee of Ministers on 28 May 2003).

[110] Zoning at the State of destination is perhaps generally marginally less harmful in terms of preserving the Internet as a transnational medium than voluntary zoning by prudent content providers, as the effect of the former, in contrast to the latter, is limited to the State imposing such censorship and tends to be limited to actually illegal material.

requirements. Yet, that does not mean that these laws are in any way ill-founded, and even in respect of cyberspace their *prima facie* legitimacy stands.

What has changed is that the online context magnifies the censorship effect, both apparent and real, of these traditional national law restrictions. This is partly because there is much less 'quiet' self-censorship, particularly by foreign providers (requiring potentially more drastic blocking actions by States), and partly because different foreign speech standards (both stricter and looser) raise a self-consciousness about one's own standards and invariably question the legitimacy of one's speech restrictions. However, the main reason for the magnified restrictive effect of traditional national law in cyberspace is what lies at the heart of the chapter: it forecloses an open Internet and open transnational communications.[111] National legal standards that seemed and were entirely legitimate, no longer appear quite so legitimate in the context of these consequences. The law has remained the same, but the stakes have changed. As even relatively subtle national legal differences cannot be maintained in an open online environment, is it really worth trying to insist on, and protect, these differences? This brings us to the final question and conclusion of this chapter and book: if, as is the case, one has to choose between a global Internet with free transnational communications and effective distinct national laws, what should one choose and how is one to make the choice?

4. Making the choice: a value judgment

National law or the transnational Internet – the choice may be simple, choosing is not. On the one hand, retaining open transnational communications comes at the cost of distinct national political, moral and cultural values, reflected in distinct national laws and legal diversity more generally. While legal differences may often appear relatively slight, especially amongst Western democratic States, they tend to reflect underlying differences that are deeply embedded in the national consciousness and not easily smoothed out. Recent EU harmonisation efforts in the criminal law field bear testimony to that.[112] Harmonisation

[111] Previously, national speech standards by and large applied to national communications.

[112] Martin Wasmeier and Nadine Thwaites, 'The "Battle of the Pillars": Does the European Community Have the Power to Approximate National Criminal Law' (2004) 29 *European Law Review* 613. See also Chapter 6, n. 221.

at a global scale presents obstacles of an entirely different dimension, and would often require substantial legal sacrifices States are not willing to make.

On the other hand, retaining distinct national laws (its retention assumes a certain level of effectiveness) undermines much of the Internet's great achievement and the closest we have come to the global village. As the US District Court in *ACLU* v. *Reno* said, 'a decrease in the number of speakers, speech fora, and permissible topics will diminish the worldwide dialogue that is the strength and signal achievement of the medium'.[113] Applying 'only' existing legal restrictions to online activity, if they are to be at all effective, necessarily chills transnational communications, and not insignificantly so. In respect of some online activity, such as the distribution of child pornography, this chilling effect may be exactly what is desired, but in respect of other activity it may not. For example, the High Court of Australia by, insisting on the application of Australian defamation law in respect of Internet publication, created a simple choice for the US defendant, assuming it took the judgment seriously:[114] either comply with the stricter Australian defamation law thereby depriving all US and other subscribers of substantive content, or cancel the Australian subscriptions thereby depriving Australians of those transnational communications. Both options necessarily have a chilling effect much greater, it seems, than that intended or justified. The repercussions of this choice become more chilling still when one considers, first, the number of other States claiming a right to protect their distinct national laws and their variety, and, secondly, the number of players that are in Dow Jones' shoes and presented with the same choice.

The same State may make different regulatory choices with regard to different types of online activity, thereby creating both room for open transnational communications and distinct national laws running concurrently in respect of different activities. For example, the UK may be willing to tolerate harmonisation at the lowest common denominator in respect of online gambling activity, but not online pornography; Germany may be willing to tolerate foreign spam, but not online hate speech. The problem is that such neat separation between regulatory areas cannot

[113] *ACLU* v. *Reno*, 929 F Supp 824, 879 (ED Pa 1996).

[114] *Dow Jones & Co. Inc.* v. *Gutnick* [2002] HCA 56. If the foreign defendant did not take the judgment seriously, the court's intention of upholding the local law would be defeated, but for the symbolic value of the judgment.

always be transplanted to online activity itself. For example, an online portal may attract a whole host of different laws, from defamation, advertising and product safety laws to privacy laws and licensing requirements. If such business would decide to avoid strict foreign licensing requirements by territorially sealing its site, more generous stances in respect of all the other substantive laws would be foregone.

How should States decide? This comes down to a matter of priorities; what is more important: open transnational communication or the retention of distinct national laws? This question cannot be decided by legal arguments or doctrines. It is a matter of value judgment, with weighty factors speaking in favour of either side. Legal arguments are of no assistance. Law may help to implement the choice made and technical measures and tools may help to implement the legal provisions, but neither law nor technology can relieve policy-makers of the initial value judgment.

Without being conclusively in favour of either, it seems that sometimes transnational communications should indeed be curtailed to protect the most fundamental values of a State, such as human dignity or the protection of the most vulnerable members of society. Conversely, transnationality should not be compromised because of national legal pettiness. But of course, in many ways this simply begs the question: when is a State's insistence on its national law a legitimate expression of its commitment to its most cherished values and when is it an expression of a nationalistic and uncooperative stance? This question cannot be answered here, but it is asserted that States ought to examine their national legal stances afresh in the harsh light of the online reality. Given the serious repercussions of holding onto one's own distinct legal standards for both the online world and national legal spaces (mainly in the form of default harmonisation), national law can no longer be treated with quite the same preciousness as previously.

Ultimately, doubts as to whether national legal standards should or should not give way to the pressure of the transnational Internet ought to be resolved in favour of free communications. As MacCormick said:

> A community of mutually respectful and self-respecting citizens would be one within which freedom of communication between and among persons would be both maximized and most of all at a premium . . . Freedom of communication is the antithesis of manipulation – so here again, the case for the Rule of Law comes down to and rests upon the value of

> respect for persons and its particular corollary of the desirability of maximal unimpeded intercommunication among persons.[115]

Finally, the following words by Fuller, written long before the Internet, eloquently capture the spirit with which the Internet ought to be endorsed by all concerned – States, politicians, judges, legislators, academics and online participants themselves:

> if we were forced to select the principle that supports and infuses all human aspiration we would find it in the objective of maintaining communication with our fellows . . . In the first place . . . man has been able to survive up to now because of his capacity for communication . . . If in the future man succeeds in surviving his own powers of self-destruction, it will be because he can communicate and reach understanding with his fellows . . . Communication is something more than a means of staying alive. It is a way of being alive. It is through communication that we inherit the achievements of past human efforts . . . How and when we accomplish communication with one another can expand or contract the boundaries of life itself. In the words of Wittgenstein, 'The limits of my language are the limits of my world.' If I were asked, then, to discern one central indisputable principle of what may be called substantive natural law . . . I would find it in the injunction: Open up, maintain, and preserve the integrity of the channels of communication by which men convey to one another what they perceive, feel, and desire.[116]

[115] Neil MacCormick, *Questioning Sovereignty* (Oxford: Oxford University Press, 1999), 46f.
[116] Lon L. Fuller, *The Morality of Law* (revised edn, New Haven: Yale University Press, 1964), 185f.

BIBLIOGRAPHY

'Is Zippo's Sliding Scale a Slippery Slope of Uncertainty? A Case for Abolishing Web Site Interactivity as a Conclusive Factor in Assessing Minimum Contacts in Cyberspace' (2001) 34 *John Marshall Law Review* 1051 (note)

'No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet' (2003) 116 *Harvard Law Review* 1821 (note)

Aarnio, Aulis and MacCormick, Neil (eds.), *Legal Reasoning* (New York: New York University Press, 1992)

Aciman, Carole and Vo-Verde, Diane, 'Refining the Zippo Test: Trends on Personal Jurisdiction for Internet Activities' (2002) 19 *Computer and Internet Lawyer* 16

Ahlert, Christian, 'Technology of Control: How Code Controls Communication', in Organization for Security and Co-operation in Europe (OSCE) (Christiane Hardy and Christian Möller eds.), *Spreading the Word on the Internet* (Vienna: OSCE, 2003), 119

Akehurst, Michael, 'Jurisdiction in International Law' (1972–3) 46 *British Yearbook of International Law* 145

Albrecht, A. R., 'The Enforcement of Taxation under International Law' (1953) 30 *British Yearbook of International Law* 454

Allott, P., *Eunomia: A New Order for a New World* (Oxford: Oxford University Press, 1990)

American Bar Association (ABA), http://www.abanet.org, *Addressing Disputes in Electronic Commerce – Final Report and Recommendations of the American Bar Association's Task Force on Electronic Commerce and Alternative Dispute Resolution* (August 2002)

'Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet' (2000) 55 *The Business Lawyer* 1801, http://www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf

Atiyah, P. S., *Law and Modern Society* (Oxford: Oxford University Press, 1983)

'From Principles to Pragmatism: Changes in the Function of the Judicial Process and the Law' (1980) 65 *Iowa Law Review* 1249

Aubert, Vilhelm and Eckhoff, Torstein (eds.), *Continuity and Development in Law and Society* (Oslo: Scandinavian University Press, 1989)

Ausness, Richard C., 'The Application of Product Principles to Publishers of Violent or Sexually Explicit Material' (2000) 52 *Florida Law Review* 603

Austin, John, *The Province of Jurisprudence Determined* (1832, ed. by H. L. A. Hart, London: Weidenfeld & Nicolson, 1954)

Australian Competition and Consumer Commission, http://www.accc.gov.au, *The Global Enforcement Challenge: Enforcement of Consumer Protection Laws in a Global Marketplace*, Discussion Paper (1997)

'ACCC Issues Warning to On-line Traders: "Shape-up" Sites' (2004)

Australian Law Reform Commission, http://www.alrc.gov.au, *Legal Risk in International Transactions*, Report No. 80 (1996)

Choice of Law, Report No. 58. (1992)

Australian Minister for Communications, Information Technology and the Arts, *Six-Month Report on Co-Regulatory Scheme for Internet Content Regulation January to June 2001* (February 2002)

Australian National Office for the Information Economy (now the Australian Government Information Management Office), http://www.agimo.gov.au, *Convergence Review – Final Review* (10 May 2000)

Australian Securities and Investments Commission, http://www.asic.gov.au *Electronic Prospectuses*, Policy Statement 107 (18 September 1996, reissued 10 February 2000)

Investment Advisory Services: Media, Computer Software and Internet Advice, Policy Statement 118 (3 March 1997, reissued 12 January 2000)

Offers of Securities on the Internet, Policy Statement 141 (10 February 1999, reissued 2 March 2000)

Australian Standing Committee of Attorneys-General (SCAG) Working Group of State and Territory Officers, *Proposal for Uniform Defamation Laws* (July 2004)

Australian Tax Office, http://www.ato.gov.au, *Tax and the Internet*, Discussion Report of the ATO Electronic Commerce Project (1997)

Axelrod, Robert, *The Complexity of Cooperation* (Princeton: Princeton University Press, 1997)

The Evolution of Co-operation (first published 1984, London: Penguin Books, 1990)

Ayres, Ian and Braithwaite, John, *Responsive Regulation – Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992)

Ayres, Phil, 'Prescribing a Cure for Online Pharmacies' (2005) 72 *Tennessee Law Review* 949

Baade, Hans W., 'The Operation of Foreign Public Law' (1995) 30 *Texas International Law Journal* 429

Balda, Volker and Schmits, Volker, 'Fernsehen ohne Grenzen auf dem Weg zur Konvergenz' (1998) 7 *Computer und Recht* 421

Baldwin, Robert, Scott, Colin and Hood, Christopher (eds.), *A Reader on Regulation* (Oxford: Oxford University Press, 1998)

Bales, Richard A. and Van Wert, Suzanne, 'Internet Jurisdiction' (2001) 20 *John Marshall Journal of Computer and Information Law* 21

Balganesh, Shyamkrishna, 'Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass' (2006) 12 *Michigan Telecommunications and Technology Law Review* 265

Barnett, Randy E., 'Forewords: Four Senses of the Public Law–Private Law Distinction' (1994) 9 *Harvard Journal of Law and Public Policy* 267

Beech, Andrew, 'Discretion in the Exercise of Jurisdiction: Recent Developments' (1989) 19 *University of Western Australia Law Review* 8

Bell, Griffin B., 'International Comity and the Extra-territorial Application of Anti-Trust Laws' (1977) 51 *Australian Law Journal* 80

Benkler, Yockai, 'Internet Regulation: A Case Study on the Problem of Unilateralism' (2000) 11 *European Journal of International Law* 171

Bentham Jeremy, *Of Laws in General* (ed. by H. L. A. Hart, London: Athlone Press, 1970)

Berman, Paul Schiff, 'The Globalisation of Jurisdiction' (2002) 151 *University of Pennsylvania Law Review* 311

Bernardez, Santiago Torres, 'Territorial Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 487

Betlem, Gerrit, 'Cross-Border Private Enforcement of Community Law', in J. A. E. Vervaelde (ed.), *Compliance and Enforcement of European Community Law* (The Hague: Kluwer Law International, 1999), 391

'Transboundary Enforcement: Free Movement of Injunction', in Sven Deimann and Bernard Dyssli (eds.), *Environmental Rights – Law, Litigation and Access to Justice* (London: Cameron May, 1995), 184

Betlem, Gerrit and Nollkaemper, Andre, 'Giving Effect to Public International Law and European Community Law before Domestic Courts: A Comparative Analysis of the Practice of Consistent Interpretation' (2003) 14 *European Journal of International Law* 567

Beyleveld, Deryck, Kirkham, Richard and Townend, David, 'Which Presumption? A Critique of the House of Lords' Reasoning on Retrospectivity and the Human Rights Act' (2002) 22 *Legal Studies* 185

Bigos, Oren, 'Jurisdiction over Cross-Border Wrongs on the Internet' (2005) 54 *International and Comparative Law Quarterly* 585

Bowrey, Kathy, *Law and Internet Cultures* (Cambridge: Cambridge University Press, 2005)

Boyle, James, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors' (1997) 66 *University of Cincinnati Law Review* 177

Bradney, Tony, 'Law Schools and the Egg Marketing Board' (2001) 22 *SPTL Reporter* 1

Braun, Odelia, 'Internet Publications and Defamation: Why the Single Publication Rule Should Not Apply' (2002) 32 *Golden Gate University Law Review* 325

Bremer, Karsten, *Strafbare Internet-Inhalte in International Hinsicht – Ist der Nationalstaat wirklich überholt?* (Frankfurt a. M.: Peter Lang Verlag, 2001), http://ub-dok.uni-trier.de/diss/diss60/20000927/20000927.pdf

Brownlie, Ian, *Principles of Public International Law* (6th edn, Oxford: Oxford University Press, 2003)

Principles of Public International Law (4nd edn, Oxford: Clarendon Press, 1990)

Brownsword, Roger, 'Code, Control, and Choice: Why East Is East and West Is West' (2005) 25 *Legal Studies* 1

Burk, Dan L., 'Jurisdiction in a World Without Borders' (1997) 1 *Virginia Journal of Law and Technology* 1522

Burnstein, Matthew R., 'Conflicts on the Net: Choice of Law in Transactional Cyberspace' (1996) 29 *Vanderbilt Journal of Transnational Law* 75

Buxbaum, Hannah L., 'The Private Attorney General in a Global Age: Public Interests in Private International Antitrust Litigation' (2001) 26 *Yale Journal of International Law* 219

Byers, Michael, *Custom, Power and the Power of Rules* (Cambridge: Cambridge University Press, 1999)

Camp, L. Jean and Syme, Serena, 'Code as Governance, the Governance of Code' (2001), John F Kennedy School Government Faculty Research Working Paper Series, http://ssrn.com/abstract=297154/

Carr, Indira and Williams, Katherine S., 'Cyber-crime and the Council of Europe: Reflections on a Draft Convention' (2001) 7 *International Trade Law and Regulation* 93

Carter, P. B., 'Rejection of Foreign Law: Some Private International Law Inhibitions' (1984) 55 *British Yearbook of International Law* 111

Cassese, Antonio, *International Law* (Oxford: Oxford University Press, 2001)

Cohen, Laurence J., 'E-Libel and Proportionality' (2000) 1 *E-Journal* 12

Collier, J. G., *Conflict of Laws* (3rd edn, Cambridge: Cambridge University Press, 2001)

Collins, Lawrence (ed.), *Dicey and Morris on Conflict of Laws* (13th edn, London: Sweet & Maxwell, 2000)

Collins, Matthew, *The Law of Defamation and the Internet* (Oxford: Oxford University Press, 2001)

Online Updates to the Law of Defamation and the Internet, http://www.mattcollins.com.au/LawofDefamationandtheInternet.html

Corn-Revere, Robert, *Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech*, Briefing Paper No. 71 (2002), Cato Institute, http://www.cato.org/pubs/briefs/bp71.pdf

Commonwealth of Australia, *Australia–United States Relations: The Extraterritorial Application of United States Laws*, Joint Committee on Foreign Affairs and Defence (Canberra, 1983)

Commonwealth Scientific and Industrial Research Organisation (CSIRO) (Philip McCrea, Bob Smart and Mark Andrews), *Blocking Content on the Internet: A Technical Perspective* (June 1998), http://www.cmis.csiro.au/projects+sectors/blocking.pdf

Council of Europe, http://www.coe.int, *Declaration on Freedom of Political Debate in the Media* (adopted by the Committee of Ministers on 12 February 2004)

Declaration on Freedom of Communication on the Internet (adopted by the Committee of Ministers on 28 May 2003)

Draft Declaration on Freedom of Communication on the Internet (8 April 2002)

Recommendation No. R(97)20E of the Committee of Ministers to Member States on 'Hate Speech' (adopted by the Committee of Ministers on 30 October 1997)

Currie, Brainerd, *Selected Essays in the Conflict of Laws* (Cambridge: Cambridge University Press, 1963)

Davies, Martin, Ricketson, Sam and Lindell, Geoffrey, *Conflicts of Laws – Commentary and Materials* (Sydney: Butterworths, 1997)

Davis, Phillip Adam, 'The Defamation of Choice-of-Law in Cyberspace: Countering the View that the Restatement (Second) of Conflict of Laws Is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier' (2002) 54 *Federal Communications Law Journal* 339

Deakin, Simon, *Legal Diversity and Regulatory Competition: Which Model for Europe?* Working Paper No. 323 (Centre for Business Research, University of Cambridge, 2006), http://www.cbr.cam.ac.uk/pdf/WP323.pdf

International and Jurisdictional Issues (ESRC Centre for Business Research, University of Cambridge, 1999)

Debussere, Frederic, 'International Jurisdiction over E-Consumer Contracts in the European Union: Quid Novi Sub Sole?' (2002) 10 *International Journal of Law and Information Technology* 344

Dennis, Everette E., 'Internal Examination: Self-Regulation and the American Media' (1995) 13 *Cardozo Arts and Entertainment Law Journal* 697

Dewey, John, 'Logical Method and Law' (1924) 10 *Cornell Law Quarterly* 17

Dinwoodie, Graeme, 'Trademarks and Territory: Detaching Trademark from the Nation-State' (2004) 41 *Houston Law Review* 885

Dodge, William S., 'Antitrust and the Draft Hague Judgments Convention' (2001) 33 *Law and Policy in International Business* 363

'Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism' (1998) 39 *Harvard International Law Journal* 101

Doehring, Karl, 'State', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 423

Donaghey, Teague I., 'Terminal Railroad Revisited: Using the Essential Facilities Doctrine to Ensure Accessibility to Internet Software Standards' (1997) 25 *AIPLA Quarterly Journal* 277

Doughdrill, Brian E., 'Personal Jurisdiction and the Internet: Waiting for the Other Shoe to Drop on First Amendment Concern' (2000) 51 *Mercer Law Review* 919

Dyson, George, *Darwin Among the Machines* (London: Allen Lane, 1998)

Edelman, Benjamin (Berkman Center for Internet and Society, http://cyber.law.harvard.edu/home/), *Empirical Analysis of Google SafeSearch* (2003), Berkman Center for Internet & Society

Web Sites Sharing IP Addresses: Prevalence and Significance (2003), Berkman Center for Internet and Society

'Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users' (Expert Memorandum attached to the National Association of Broadcasters' submission to Industry Canada) (2001)

Eden, Sandra, 'Taxation of Electronic Commerce', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet – Regulating Cyberspace* (Oxford: Hart Publishing, 1997), 151

Edwards, Lilian, 'Defamation and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet – Regulating Cyberspace* (Oxford: Hart Publishing, 1997), 183

Eko, Lyombe, 'Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation' (2001) 6 *Communication Law and Policy* 445

Eorsi, Gyula, *Comparative Civil (Private) Law* (Budapest: Academiai Kiado, 1979)

European Commission, http://ec.europa.eu, *Special Eurobarometer 250 'Safer Internet' Report* (May 2006)

Safer Internet Plus Programme, Factsheet 18 (October 2005), *Communication on the Mutual Recognition of Judicial Decisions in Criminal Matters and the Strengthening of Mutual Trust between Member States*, COM(2005) 195 final

Green Paper on Conflicts of Jurisdiction and the Principle of Ne Bis in Idem in Criminal Proceedings, COM(2005) 696 final

Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument and its Modernisation, COM(2002) 654 final

Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee: Electronic Commerce and Indirect Taxation, COM(1998) 374 final

Farber, Daniel A., 'Expressive Commerce in Cyberspace: Public Goods, Network Effects and Free Speech' (2000) 16 *Georgia State University Law Review* 789

Faulstich, Werner, 'Mediengeschichte', in Werner Faulstich (ed.), *Grundwissen Medien* (Munich: Wilhelm Fink Verlag, 1994), 19

Fawcett, James J. and Torremans, Paul, *Intellectual Property and Private International Law* (Oxford: Oxford University Press, 1998)

Feintuck, Mike, *Media Regulation, Public Interest and the Law* (Edinburgh: Edinburgh University Press, 1999)

Feld, Harold, 'Structured to Fail: ICANN and the Privatisation Experiment', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net?* (Washington DC: Cato Institute, 2003), 333

Feldman, David, *Civil Liberties and Human Rights in England and Wales* (2nd edn, Oxford: Oxford University Press, 2002)

Feng, Zhen, 'China to Introduce New Legislation to Deal with ISP Liability for Copyright Infringement' (2004) 5 *World Internet Law Report* 19

Ferguson, Niall, *The Cash Nexus: Money and Power in the Modern World 1700–2000* (London: Allen Lane, 2001)

Ferran, Eilis, *Company Law and Corporate Finance* (Oxford: Oxford University Press, 1999)

Fitzmaurice, G., 'The General Principles of International Law Considered from the Standpoint of the Rule of Law' (1957) 92 *Recueil des Cours* 209

Fleming, John G., *The Law of Torts* (9th edn, Sydney: LBC Information Services, 1998)

Foss, M. and Bygrave, L. A., 'International Consumer Purchases through the Internet: Jurisdictional Issues Pursuant to European Law' (2000) 8 *International Journal of Law and Information Technology* 99

Franklin, Marc A., Anderson, David and Cate, Fred H., *Mass Media Law* (6th edn, New York: Foundation Press, 2000)

Freeman, D. A., 'Milgram's Obedience to Authority – Some Lessons for Legal Theory' (1979) 1 *Liverpool Law Review* 45

Fromme, Friedrich Karl and Dornhege, Hermann, '"Die Entscheiding is unanfechtbar" Das Bundesverfassungsgericht' (1997) 6 *Deutschland – Zeitschrift fuer Politik, Kultur, Wirtschaft und Wissenschaft* 24

Frowein, Jochen, 'Recognition', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 340

Fuller, Lon L., *The Morality of Law* (New Haven: Yale University Press, 1964)

Garnett, Richard, 'Trademarks and the Internet: Resolution of International IP Disputes by Unilateral Application of US Law' (2005) 30 *Brooklyn Journal of International Law* 925

'Dow Jones & Company Inc v Gutnick – An Adequate Response to Transnational Internet Defamation?' (2003) 4 *Melbourne Journal of International Law* 197

'International Arbitration Law: Progress Towards Harmonisation' (2002) 3 *Melbourne Journal of International* Law 400

'Are Foreign Internet Infringers beyond the Reach of the Law?' (2000) 23 *University of New South Wales Law Journal* 105

'Regulating Foreign-Based Internet Content: A Jurisdictional Perspective' (2000) 6 *University of New South Wales Law Journal* 8

Geist, Michael, 'Is There a There There? Towards Greater Certainty for Internet Jurisdiction' (2001) 661 *PLI/Pat* 561

Gladwell, Malcolm, *The Tipping Point* (London: Abacus, 2001)

Goldsmith, Jack, 'Unilateral Regulation of the Internet: A Modest Defence' (2000) 11 *European Journal of International Law* 135

'The Internet and the Abiding Significance of Territorial Sovereignty' (1998) 5 *Indiana Journal of Global Legal Studies* 475

'What Internet Gambling Legislation Teaches About Internet Regulation' (1998) 32 *The International Lawyer* 1115

Goode, Matthew, 'The Tortured Tale of Criminal Jurisdiction' (1997) 21 *Melbourne University Law Review* 411

Goodhart A. L., *English Law and the Moral Law System* (London: Stevens & Son, 1953)

Goodman, Marc D. and Brenner, Susan, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10 *International Journal of Law and Information Technology* 139

Grabosky, P. N. and Smith, Russell G., *Crime in the Digital Age* (Leichhardt, NSW: Federation Press, 1998)

Graveson, R. H., *Comparative Conflict of Laws* (Oxford: North-Holland Publishing Company, 1977)

Greig, Donald W. 'Sources of International Law', in Sam Blay, Ryszard Piotrowicz and Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005)

Greve, Michael S., 'If It Ain't Broke, Why Is Everyone Trying to Fix It? Taxing E-Commerce in a Destination-Based World', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: Cato Institute, 2003), 269

Griffith, Gareth, *Censorship in Australia: Regulating the Internet and other Recent Developments*, Briefing Paper (April 2002)

Gringas, Clive, *The Laws of the Internet* (London: Butterworths, 1997)

Gross, Grant, 'US Anti-Spam Law Still Not Making a Difference' (2 April 2004), Techworld, http://www.techworld.com/security/news/index.cfm?newsid=1332/.

Gross, Jason, 'Internet Gambling and the Law – Prohibition vs. Regulation' (August 2006) *The Metropolitan Corporate Counsel* 2, http://www.metrocorpcounsel.com/pdf/2006/August/11.pdf

Hague Conference on Private International Law, http://www.hcch.net (Andrea Schulz), *Proceedings of the International Conference on the Legal Aspect of an E-Commerce Transactions* (2004)

(Avril D. Haines), *The Impact of the Internet on the Judgments Projects: Thoughts for the Future*, Prel. Doc. No. 17 (2002)

(Catherine Kessedjian), *Electronic Commerce and International Jurisdiction*, Prel. Doc. No. 12 (2000)

(Peter Nygh and Fausto Pocar), *Report of the Special Commission*, Prel. Doc. No. 11 (1999)

Hancher, L. and Moran, M., 'Organizing Regulatory Space', in Robert Baldwin, Colin Scott and Christopher Hood (eds.), *A Reader on Regulation* (Oxford: Oxford University Press, 1998), 148

Harding, Christopher, 'Legal Subjectivity as a Fundamental Value: The Emergence of Non-State Actors in Europe', in Kim Economides *et al.* (eds.), *Fundamental Values* (Oxford: Hart Publishing, 2000), 115

'The Identity of European Law: Mapping Out the European Legal Space' (2000) 6 *European Law Journal* 128

Hardy, I. Trotter, 'The Proper Legal Regime for "Cyberspace"' (1994) 55 *University of Pittsburgh Law Review* 995

Harris, David J., *Cases and Materials on International Law* (5th edn, London: Sweet & Maxwell, 1998)

Hart, H. L. A., *The Concept of Law* (1961, 2nd edn, Oxford: Clarendon Press, 1994)

Essays on Bentham (Oxford: Clarendon Press, 1982)

The Province of Jurisprudence Determined (London: Weidenfeld & Nicolson, 1954)

Hawkins, Keith, *Environment and Enforcement: Regulation and the Social Definition of Pollution* (Oxford: Clarendon Press, 1984)

Hestermeyer, Holger P., 'Personal Jurisdiction for Internet Torts: Towards an International Solution' (2006) 26 *Northwestern Journal of International Law and Business* 267

Higgins, Rosalyn, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon Press, 1994)

'The Legal Bases of Jurisdiction', in Cecil J. Olmstead (ed.), *Extraterritorial Application of Laws and Responses Thereto* (Oxford: ECS Publishing Limited, 1984), 3

Hirst, Michael, 'Cyberobscenity and the Ambit of Criminal Law' (2002) 13 *Computers & Law* 25

Holder, William E., 'Public Policy and National Preferences: The Exclusion of Foreign Law in English Private International Law' (1969) 17 *International and Comparative Law Quarterly* 926

Hörnle, Julia, 'Country of Origin Regulation in Cross-Border Media: One Step Beyond the Freedom to Provide Services?' (2005) 54 *International and Comparative Law Quarterly* 89

'Online Dispute Resolution in Business to Consumer E-Commerce Transactions' (2002) (2) *Journal of Information, Law and Technology*

Hurt, Christine, 'Regulating Public Morals and Private Markets: Online Securities Trading, Internet Gambling and the Speculation Paradox' (2005) 86 *Boston University Law Review* 371

International Chamber of Commerce, http://www.iccwbo.org, *The Impact of Internet Content Regulation* (18 November 2002)

Jurisdiction and Applicable Law in Electronic Commerce (6 June 2001)

International Law Association, http://www.ila-hg.org, *First Report by the Committee on Transnational Enforcement of Environmental Law* (2002)

International Telecommunication Union (ITU), http://www.itu.int, *ITU Survey on Anti-Spam Legislation Worldwide* (2005) CYB/06

Jacobson, Joy, 'Of Love and Defamation in China' (2003) *Poets & Writers Magazine*, http://www.pw.org

Jennings, Robert and Watts, Arthur (eds.), *Oppenheim's International Law* (9th edn, London: Longman, 1992)

Johnson, David R. and Post, David, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367

Kaiser, Karl, 'Wie das Internet die Weltpolitik verandert' (2001) 3 *Deutschland – Zeitschrift fuer Politik, Kultur, Wirtschaft und Wissenschaft* 40

Kalathil, Shanthi and Boas, Taylor C., 'The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution' (2001) Carnegie Endowment Working Papers, Global Policy Program No 21, http://www.carnegieendowment.org/files/21KalathilBoas.pdf

Katsh, Ethan, 'Cybertime, Cyberspace and Cyberlaw' (1995) *Journal of Online Law*

Katyal, Neal Kumar, 'Digital Architecture as Crime Control' (2003) 112 *Yale Law Journal* 2261

Kearsly, Amanda, 'The Internet, Paedophilia and the ISP' (2001) April/May *Computers and Law* 29

Keck, Richard, 'Developing an Intuitive Understanding of the Behavior and Legal Treatment of Information Assets' (2001) 605 *PLI/Pat* 771

Kelsen, Hans, *General Theory of Law and State* (Cambridge, MA: Harvard University Press, 1946)

Kightlinger, Mark F., 'A Solution to the *Yahoo!* Problem? The EC E-Commerce Directive as a Model for International Cooperation on Internet Choice of Law' (2003) 24 *Michigan Journal of International Law* 719

Kohl, Uta, 'Ignorance Is No Defence But Is Inaccessibility? On the Accessibility of Law in the Transnational Online Context' (2005) 14 *Information & Communications Technology Law* 27

'Who Has the Right to Govern Online Activity? A Criminal and Civil Point of View' (2004) 18 *International Review of Law, Computers and Technology* 387

'The Rule of Law, Jurisdiction and the Internet' (2004) 12 *International Journal of Law and Information Technology* 365

'Defamation on the Internet – Nice Decision, Shame about the Reasoning. Dow Jones & Co v Gutnick' (2003) 52 *International and Comparative Law Quarterly* 1049

'Eggs, Jurisdiction and the Internet' (2002) 51 *International and Comparative Law Quarterly* 555

'Yahoo! – But No Hooray! for the International Online Community' (2001) 75 *Australian Law Journal* 411

'Defamation on the Internet – A Duty Free Zone After All? Macquarie Bank Ltd & Anor v Berg' (2000) 22 *Sydney Law Review* 119

'Legal Reasoning and Legal Change in the Age of the Internet – Why the Ground Rules Are Still Valid' (1999) 7 *International Journal of Law and Information Technology* 123

Kramer, Larry, 'Rethinking Choice of Law' (1990) 90 *Columbia Law Review* 277

Kress, Claus, 'Universal Jurisdiction over International Crimes and the Institut de Droit international' (2006) 4 *Journal of International Criminal Justice* 561

Kuchinskas, Susan, 'Google Axes Hate News' (23 March 2005), Internetnews.com, http://www.internetnews.com/xSP/article.php/3492361/

Lasswell, Harold D., 'The Structure and Function of Communication in Society', in Wilbur Schramm (ed.), *Mass Communications* (2nd edn, Urbana: University of Illinois Press, 1960), 117

Lauterbach, H., 'The Problem of Jurisdictional Immunities of Foreign States' (1951) 28 *British Yearbook of International Law* 220

Leets, Laura, 'Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace?' (2001) 6 *Communication Law and Policy* 287

Lemley, Mark A. and McGowan, David, 'Legal Implications of Network Economic Effects' (1998) 86 *California Law Review* 479

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501

'The Laws of Cyberspace – Draft 3' (1998), http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf

'The Zones of Cyberspace' (1996) 48 *Stanford Law Review* 1403

Levinson, L. Harold, 'The Public Law/Private Law Distinction in the Courts' (1989) 57 *George Washington Law Review* 1579

Levinson, Paul, *Digital McLuhan – A Guide to the Information Millennium* (London: Routledge, 1999)

The Soft Edge – A Natural History and Future of the Information Revolution (London: Routledge, 1997)

Lianos, Michalis, 'Social Control after Foucault' (2003) 1(3) *Surveillance and Society* 412

Lombois, Claude, *Droit Penal International* (2nd edn, Paris: Dalloz, 1979)

Lowe, A. V. (ed.), *Extraterritorial Jurisdiction – An Annotated Collection of Legal Materials* (Cambridge: Grotius Publications Ltd, 1983)

Lowenfeld, Andreas F., 'Public Law in the International Arena: Conflict of Laws, International Law and Some Suggestions for their Interaction' (1979) 163 *Recueil des Cours* 311

Luban, David, 'The Publicity of Law and the Regulatory State' (2002) 10 *Journal of Political Philosophy* 296

MacCormick, Neil, *Questioning Sovereignty* (Oxford: Oxford University Press, 1999)

Legal Reasoning and Legal Theory (first published 1978, Oxford: Oxford University Press, 1994)

'The Artificial Reason and Judgement of Law', in Aulis Aarnio and Neil MacCormick (eds.), *Legal Reasoning* (New York: New York University Press, 1992), Vol. 1, 167

'On Legal Decisions and Their Consequences: From Dewey to Dworkin' (1983) 58 *New York University Law Review* 239

Legal Right and Social Democracy: Essays in Legal and Political Philosophy (Oxford: Oxford University Press, 1982)

MacQueen, Hector, 'Copyright and the Internet', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet – A Framework for Electronic Commerce* (2nd edn, Oxford: Hart Publishing, 2000), 67

Maggs, Peter B., 'Abusive Advertising on the Internet (Spam) under United States Law' (2006) 54 *American Journal of Comparative Law* 385

Magnus, Ulrich and Mankowski, Peter, *Joint Response to the Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument and its Modernisation COM(2002) 654 final* (2003), http://ec.europa.eu/justice_home/news/consulting_public/rome_i/news_summary_rome1_en.htm

Maltby, Jeremy, 'Juggling Comity and Self-Government: The Enforcement of Foreign Libel Judgments in US Courts' (1994) 94 *Columbia Law Review* 1978

Mann, F. A., *Further Studies in International Law* (Oxford: Clarendon Press, 1990)

'The Doctrine of International Jurisdiction Revisited After Twenty Years' (1984) 186 *Recueil des Cours* 9

'Conflicts of Laws and Public Law' (1971) 132 *Recueil des Cours* 107

'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recueil des Cours* 1, reproduced in F. A. Mann, *Studies in International Law* (Oxford: Clarendon Press, 1973)

Mann, Michael, 'Foreign Revenue Laws and the English Conflict of Laws' (1954) 8 *International and Comparative Law Quarterly* 465

Mathiason, John R. and Kuhlman, Charles C., *An International Communication Policy: The Internet, International Regulation and New Policy Structures* (1998), http://www.intlmgt.com/portfolio/ITSpaper.html

Max Planck Institute for Foreign Private and Private International Law, *Comments on the European Commission's Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument* (2003), http://ec.europa.eu/justice_home/news/consulting_public/rome_i/news_summary_rome1_en.htm

Mayer, Franz C., 'Recht und Cyberspace' (1997) 3 *Humboldt Forum Recht*, http://www.rewi.hu-berlin.de/online/hfr/3-1997/Drucktext.html

McConnaughay, Philip J., 'Reviving the "Public Law Taboo" in the International Conflicts of Law' (1999) 35 *Stanford Journal of International Law* 255

McCorquodale, Robert and Pangalangan, Raul, 'Pushing Back the Limitations of Territorial Boundaries' (2001) 12 *European Journal of International Law* 867

McGuire, John F., 'When Speech is Heard Around the World: Internet Content Regulation in the United States and Germany' (1999) 74 *New York University Law Review* 750

McMahon, Tom, 'Improving Access to the Law in Canada' (1999) *Computerisation of Law Resources* 3

Meessen, Karl M., 'International Law Limitations on State Jurisdiction', in Cecil J. Olmstead (ed.), *Extra-Territorial Application of Laws and Responses Thereto* (Oxford: ESC Publishing Limited, 1984), 38

Mefford, Aron, 'Lex Informatica: Foundations of Law on the Internet' (1997) 5 *Indiana Journal of Global Legal Studies* 211

Mehra, Salil K., 'Deterrence: The Private Remedy and International Antitrust Cases' (2002) 40 *Columbia Journal of Transnational Law* 275

Meng, Werner, 'Recognition of Foreign Legislative and Administrative Act', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 348

Meron, Theodor, *Human Rights and Humanitarian Norms as Customary Law* (Oxford: Oxford University Press, 1989)

Merryman, John Henry, 'The Public Law–Private Law Distinction in European and American Law' (1968) 17 *Journal of Public Law* 2

Metzger, R. S., 'Communications Convergence' (2001) 18 *Computer and Internet Lawyer* 1

Meyer, Christopher W., 'World Wide Web Advertising: Personal Jurisdiction Around the Whole Wide World?' (1997) 54 *Washington and Lee Law Review* 1269

Milgram, Stanley, *Obedience to Authority* (London: Tavistock, 1974)

Miller, Nigel, 'Has Your Trademark Been Googled?' (2004) 15 *Computer & Law* 36

Mnookin, Robert H., 'The Public/Private Dichotomy: Political Disagreement and Academic Repudiation' (1982) 130 *University of Pennsylvania Law Review* 1429

Mody, Sanjay S., 'National Cyberspace Regulation: Unbundling the Concept of Jurisdiction' (2001) 37 *Stanford Journal of International Law* 365

Moerel, Lokke, 'The Country-of-Origin Principle in the E-Commerce Directive: The Expected One Stop Shop' (2001) 7 *Computer and Telecommunication Law Review* 184

Mozina, Damjan, 'Persönlichkeitsverletzungen im Internet – Die Internationale Zuständigkeit' (2004) 1 *Slovenian Law Review* 77

Muchlinski, Peter Thomas, 'Globalisation and Legal Research' (2003) 37 *International Lawyer* 221

Mutz, Gerfried, 'Private International Law', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 330

Naughton, John, *A Brief History of the Future – The Origins of the Internet* (London: Phoenix, 2000)

Netanel, Neil Weinstock, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 *California Law Review* 395

Nguy, N., 'Using Architectural Constraints and Game Theory to Regulate International Cyberspace Behaviour' (2004) 5 *San Diego International Law Journal* 431

Nguyen, Titi, 'A Survey of Personal Jurisdiction Based on Internet Activity: A Return to Tradition' (2004) 19 *Berkeley Technology Law Journal* 519

Nitschke, Paul and Griggs, Lynden, 'Banking on the Internet – Reformulation of the Old or Adoption of the New' (1996) 7 *Journal of Law and Information Science* 223

North, Peter and Fawcett, J. J., *Cheshire and North's Private International Law* (13th edn, London: Butterworths, 1999)

Nygh, P. N., *Conflicts of Law in Australia* (6th edn, Sydney: Butterworths, 1995)

Online Policy Group Inc, *Why Blocking Technology Can't Work*, http://www.onlinepolicy.org/research/blockcantwork.shtml

Oren, Joakim S. T., 'International Jurisdiction over Consumer Contracts in e-Europe' (2003) 52 *International and Comparative Law Quarterly* 665

Organization for Economic Co-operation and Development (OECD), http://www.oecd.org, *Anti-Spam Regulation* (2005) DSTI/CP/ICCP/SPAM(2005)10/FINAL

OECD Input to the United Nations Working Group on Internet Governance (WGIG) (2005) DSTI/ICCP(2005)4/FINAL

The Use of Authentication Across Borders in OECD Countries (2005) DSTI/ICCP/REG(2005)4/FINAL

OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003)

Legal Provisions Related to Business-to-Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection (2002) DSTI/ICCP/REG/CP(2002)1/FINAL

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2002)

Measuring the Information Economy (2002)

OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)

Opeskin, Brian R., 'The Price of Forum Shopping: A Reply to Professor Juenger' (1994) 16 *Sydney Law Review* 14

Organization for Security and Co-operation in Europe (OSCE), http://www.osce.org, *Amsterdam Recommendations on Freedom of the Media and the Internet* (Vienna: OSCE, 2003)

(Christiane Hardy and Christian Möller), *Spreading the Word on the Internet* (Vienna: OSCE, 2003)

Osborne, Dawn, 'Jurisdiction on the Internet – Not Such a Barrel of Laughs for Euromarket!' (2000) August/September *Computer and Law* 26

Oxman, Bernard H., 'Jurisdiction of States', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 277

Palmer, Laura R., 'A Very Clear and Present Danger: Hate Speech, Media Reform, and Post-Conflict Democratization in Kosovo' (2001) 26 *Yale Journal of International Law* 179

Perez, Antonio F., 'The International Recognition of Judgments: The Debate between Private and Public Law Solutions' (2001) 19 *Berkeley Journal of International Law* 44

Perritt, Henry H., 'The Internet Is Changing the Public International Legal System' (2000) 88 *Kentucky Law Review* 885

'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance (1998) 5 *Indiana Journal of Global Legal Studies* 423

'Cyberspace and State Sovereignty' (1997) 3 *Journal of International Legal Studies* 155

Piotrowicz, Ryszard, 'Immunities of Foreign Ministers and their Exposure to Universal Jurisdiction' (2002) 76 *Australian Law Journal* 290

'Child Sex Tourism and Extra-Territorial Jurisdiction' (1997) 71 *Australian Law Journal* 108

Podgor, Ellen S., 'International Computer Fraud: A Paradigm for Limiting National Jurisdiction' (2002) 35 *University of California Davis Law Review* 267

Pound, Roscoe, 'Public Law and Private Law' (1939) 24 *Cornell Law Quarterly* 469

Pribetic, Antonio I., '"Strangers in a Strange Land" – Transnational Litigation, Foreign Judgment Recognition, and Enforcement in Ontario' (2004) 13 *Journal of Transnational Law and Policy* 347

Pryles, Michael C., 'Internationalism in Australian Private International Law' (1989) 12 *Sydney Law Review* 96

Puathasnanon, Sam, 'Cyberspace and Personal Jurisdiction: The Problem of Using Internet Contacts to Establish Minimum Contacts' (1998) 31 *Loyola of Los Angeles Law Review* 691

Raw, Hazel, 'Spam: Where's the Beef?' (2004) 15(1) *Computers & Law* 38

Rayfuse, Rosemary, 'International Environmental Law', in Sam Blay, Ryszard Piotrowicz and B. Martin Tsamenyi (eds.), *Public International Law – An*

Australian Perspective (2nd edn, Melbourne: Oxford University Press, 2005), 352

Raz, Joseph, 'The Rule of Law and its Virtue' (1977) 93 *Law Quarterly Review* 195
The Concept of a Legal System (Oxford: Clarendon Press, 1970)

Reed, Christopher, *Internet Law: Text and Materials* (London: Butterworths, 2000)

Reed, Kristina M., 'From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce' (2000) 13 *Transnational Lawyer* 451

Reidenberg, Joel R., 'Technology and Internet Jurisdiction' (2005) 153 *University of Pennsylvania Law Review* 1951
'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 *Texas Law Review* 553
'Governing Networks and Rule-Making in Cyberspace' (1996) 45 *Emory Law Journal* 911

Reilly, Robert, 'Mapping Legal Metaphors in Cyberspace: Evolving the Underlying Paradigm' (1998) 16 *Journal of Computer and Information Law* 579

Reiman, Mathias, 'Introduction: The *Yahoo!* Case and Conflict of Laws in the Cyberage' (2003) 24 *Michigan Journal of International Law* 663

Reiss, Albert J., 'Selecting Strategies of Social Control over Organisational Life', in K. Hawkins and J. Thomas (eds.), *Enforcing Regulation* (Boston: Kluwer-Nijhoff, 1984)

Responsible Gambling Council (Ontario), http://www.responsiblegambling.org, 'Denmark Rejects Australian Online Gambling' (16 May 2003) *Newscan*
'Law Fails to Slow Online Gambling in Australia' (8 February 2002) *Newscan*

Reydams, Luc, *Universal Jurisdiction – International and Municipal Legal Perspectives* (Oxford: Oxford University Press, 2003)

Rice, Denis T., '2001: A Cyberspace Odyssey Through US and EU Internet Jurisdiction over E-Commerce' (2001) 661 *PLI/Pat* 421

Rolph, David, 'The Message, Not the Medium: Defamation, Publication and the Internet in Dow Jones & Co Inc v Gutnick' (2002) 24 *Sydney Law Review* 263

Rotenberg, Marc, 'Fair Information Practices and the Architecture of Privacy' (2001) *Stanford Technology Law Review* 1

Rothchild, John, 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism' (1999) 74 *Indiana Law Journal* 895

Rothman, Michael S., 'It's a Small World After All: Personal Jurisdiction, the Internet and the Global Marketplace' (1999) 23 *Maryland Journal of International Law and Trade* 127

Salmony, Michael, 'Multimedia – Chancen und Illusionen – Eine kritische Betrachtung', in Michael Lehmann (ed.), *Internet- und Multimediarecht (Cyberlaw)* (Stuttgart: Schaffer-Poeschel Verlag, 1997), 1

Sanders, Jeff, 'The Extraterritorial Application of the First Amendment to Defamation' (1994) 19 *North Carolina Journal of International Law and Commercial Regulation* 515

Sassen, Saskia, 'The Impact of the Internet on Sovereignty: Unfounded and Real Worries', in Christoph Engel and Kenneth H. Keller (eds.), *Understanding the Impact of Global Networks on Local Social, Political and Cultural Values* (Baden-Baden: Nomos, 2000), 195

'Digital Networks and Power', in Mike Featherstone and Scott Lash (eds.), *Spaces of Culture – City, Nation, World* (London: Sage Publications Ltd, 1999), 49

Savigny, F. C. Von, *Private International Law: A Treatise on the Conflict of Law* (first published 1848, 2nd Guthrie trans., 1988)

Schauer, Fredrick, 'Free Speech and the Demise of the Soapbox' (1984) 84 *Columbia Law Review* 558

Schlachter, Eric, 'The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet' (1997) 12 *Berkeley Technology Law Journal* 15

Schlachter, Oscar, 'New Custom: Power, *Opinio Juris* and Contrary Practice', in Jerzy Makarczyk (ed.), *Theory of International Law at the Threshold of the 21st Century: Essays in Honour of Krzysztof Skubiszewski* (The Hague: Kluwer, 1996), 531

Schramm, Wilbur (ed.), *Mass Communications* (2nd edn, Urbana: University of Illinois Press, 1960)

Shearer, Ivan, 'Jurisdiction', in Sam Blay, Ryszard Piotrowicz and Martin Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edn, Melbourne: Oxford University Press, 2005), 154

Siebert, Fred S., 'Communications and Government', in Wilbur Schramm (ed.), *Mass Communications* (2nd edn, Urbana: University of Illinois Press, 1960), 219

Siebert, Fred S., Peterson, Theodore and Schramm, Wilbur, *Four Theories of the Press* (Urbana: University of Illinois Press, 1956)

Sinclair, Kent, 'Legal Reasoning: In Search of an Adequate Theory of Argument', in California Law Review (ed.), *Essays in Honor of Hans Kelsen* (South Hackensack, NY: Fred B. Rothman & Co, 1971)

'Legal Reasoning: In Search of an Adequate Theory of Argument' (1971) 59 *California Law Review* 821

Slutsky, Bradley A., 'Jurisdiction over Commerce on the Internet' (1996) 4 *The DataLaw Report*

Smart, P. St J., 'International Insolvency and the Enforcement of Foreign Revenue Laws' (1986) 35 *International and Comparative Law Quarterly* 704

Smith, Bradford L., 'The Third Industrial Revolution: Law and Policy for the Internet' (2000) 282 *Recueil des Cours* 229

Smith, Graham, *Internet Law and Regulation* (3rd edn, London: Sweet & Maxwell, 2002) *Online Updates to Internet Law and Regulation*, http://www.smlawpub.co.uk/online/intereg/apr02.cfm

Snijders, Henricus and Weatherill, Stephen (eds.), *E-Commerce Law: National and Transnational Topics and Perspectives* (The Hague: Kluwer Law International, 2003)

Spencer, A. Benjamin, 'Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network Mediated Contacts' (2006) *University of Illinois Law Review* 71

Spilsbury, Sallie, *Media Law* (London: Cavendish, 2000)

Stein, Allan R., 'The Unexceptional Problem of Jurisdiction in Cyberspace' (1998) 32 *The International Lawyer* 1167

Stein, Peter and Shand, John, *Legal Values in Western Society* (Edinburgh: Edinburgh University Press, 1974)

Steinberger, Helmut, 'Sovereignty', in Rudolf Bernhardt (ed.), *Encyclopaedia of Public International Law* (1987), Vol. 10, 397

Stoel, Thomas B., 'The Enforcement of Foreign Non-Criminal Penal and Revenue Judgments in England and the United States' (1967) 16 *International and Comparative Law Quarterly* 663

Stone, Julius, *The Legal Systems and Lawyer's Reasoning* (Stanford: Stanford University Press, 1964)

Stone, Peter, 'Internet Consumer Contracts and European Private International Law' (2000) 9 *Information and Communications Technology Law* 5

Stravitz, Howard B., 'Personal Jurisdiction in Cyberspace: Something More Is Required on the Electronic Stream of Commerce' (1998) 49 *South Carolina Law Review* 925

Sullivan, Danny, 'Google Now Censoring China' (25 January 2006), SearchEngineWatch, http://blog.searchenginewatch.com/blog/060125-072617/

Summers, Robert S., 'Two Types of Substantive Reasons: The Core of a Theory of Common-Law Jurisdictions' (1978) 63 *Cornell Law Review* 707

Svantesson, Dan Jerker B., 'Borders *on*, or Border *around* – The Future of the Internet' (2006) 16 *Albany Law Journal of Science and Technology* 343

'Geo-Location Technologies and other Means of Placing Borders on the 'Borderless' Internet' (2004) 23 *John Marshall Journal of Computer and Information Law* 101

Swire, Peter P., 'Of Elephants, Mice and Privacy: International Choice of Law and the Internet' (1998) 32 *The International Lawyer* 991

Taggart, Will, 'The Digital Revolt: Resistance and Agency on the Net' (2001) *New Media and Information Technology in the Middle East*, http://nmit.georgetown.edu/papers/wtaggert.htm

Teubner, Gunther, *Global Law Without a State* (Aldershot: Dartmouth, 1997)

Thornburg, Elizabeth G., 'Fast Cheap and Out of Control: Lessons from the ICANN Dispute Resolution Process' (2002) 6 *Journal of Small and Emerging Business Law* 191

'Going Private: Technology, Due Process, and Internet Dispute Resolution' (2000) 34 *UC Davis Law Review* 151

Thierer, Adam and Crews Jr, Clyde Wayne (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: Cato Institute, 2003)

Timofeeva, Yulia A., 'Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis' (2005) 20 *Connecticut Journal of International Law* 199

Trachtman, Joel P., 'Cyberspace, Sovereignty, Jurisdiction and Modernism' (1998) 5 *Indiana Journal of Global Legal Studies* 561

Trudel, Pierre, 'Jurisdiction over the Internet: A Canadian Perspective' (1998) 32 *The International Lawyer* 1027

Tschuma, Lawrence, 'Hierarchies and Governance: Competing Regulatory Paradigms in Global Economic Regulation' (2000) (1) *Law, Social Justice and Global Development*

Unger, Roberto, 'Critical Legal Studies Movement' (1983) 96 *Harvard Law Review* 561

Urquhart, Joshua G., 'Transnational Securities Fraud Regulation: Problems and Solutions' (2000) 1 *Chicago Journal of International Law* 471

UK Department for Culture, Media and Sport, http://www.culture.gov.uk, Joint Committee on the Draft Gambling Bill, *First Report* (25 March 2004)

Draft Gambling Bill – Regulatory Impact Assessment (November 2003)

The Future Regulation of Remote Gambling: A DCMS Position Paper (April 2003)

A Safe Bet for Success – Modernising Britain's Gambling Laws (March 2002)

Gambling Review Report (July 2001)

UK Department of Trade and Industry, http://www.dti.gov.uk, *Cross Border Jurisdiction FAQs* (2006)

Implementation of the Directive on Privacy and Electronic Communications (March 2003)

UK Home Office, http://www.homeoffice.gov.uk, *Review of Extra-Territorial Jurisdiction*, Steering Committee Report (1996)

UK Law Commission, http://www.lawcom.gov.uk, *Mutual Legal Assistance Guidelines: Obtaining assistance in the UK and Overseas* (2nd edn, December 2004)

Defamation and the Internet – A Preliminary Investigation, Scoping Study No. 2 (2002)

UK Office of Fair Trading, http://www.oft.gov.uk, *Cross-Border Action to Tackle Spam* (3 November 2005)

UN Conference on Trade and Development (UNCTAD), http://www.unctad.org, *E-Commerce and Development Report 2002* (UNCTAD/SDTE/ECB/2)

US Securities and Exchange Commission, http://www.sec.gov, *Statement of the Commission Regarding Use of Internet Web Sites to Offer Securities, Solicit*

Securities Transactions or Advertise Investment Services Offshore, International Series Release No. 1125 (23 March 1998)

Van Houweling, Molly S., 'Enforcement of Foreign Judgments, the First Amendment, and Internet Speech: Notes for the Next Yahoo! v. LICRA' (2003) 24 *Michigan Journal of International Law* 697

Vartanian, Thomas P., Ledig, Robert H. and Bruneau, Lynn, *21st Century Money, Banking and Commerce* (Washington DC: Fried, Frank, Harris, Shriver & Jacobson, 1998)

Vasiljeva, Ksenija, '1968 Brussels Convention and EU Council Regulation No. 44/2001: Jurisdiction in Consumer Contracts Concluded Online' (2004) 10 *European Law Journal* 123

Vassilaki, Irini E., 'Anmerkung' (2001) 4 *Computer und Recht* 262

Waelde, Charlotte, 'Trade Marks and Domain Names: What's in a Name?', in Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet – A Framework for Electronic Commerce* (2nd edn, Oxford: Hart Publishing, 2000), 133

Wasmeier, Martin and Thwaites, Nadine, 'The "Battle of the Pillars": Does the European Community Have the Power to Approximate National Criminal Law' (2004) 29 *European Law Review* 613

Watt, Horatia Muir, 'Yahoo! Cyber-Collision of Cultures: Who Regulates?' (2003) 24 *Michigan Journal of International Law* 673

Weinrib, Ernest J., *The Idea of Private Law* (Cambridge, MA: Harvard University Press, 1995)

Wildhaber, Luzius, 'The Continental Experience', in Cecil H. J. Olmstead (ed.), *Extraterritorial Application of Laws and Responses Thereto* (Oxford: ECS Publishing Limited, 1984), 63

Williams, Cynthia A., 'Corporate Compliance with the Law in the Era of Efficiency' (1998) 76 *North Carolina Law Review* 1265

Williams, Glanville, 'The Venue and Ambit of the Criminal Law' (1965) 81 *Law Quarterly Review* 518

Wilske, Stephan and Schiller, Terasa, 'International Jurisdiction in Cyberspace: Which States May Regulate the Internet?' (1997) 50 *Federal Communications Law Journal* 117

Wimmer, Kurt, 'International Liability for Internet Content: Publish Locally, Defend Globally', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net?* (Washington DC: Cato Institute, 2003), 239

Winn, Jane Kaufman, 'The Hedgehog and the Fox: Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions' (1999) 51 *Administrative Law Review* 955

World Trade Organization (WTO), http://www.wto.org, *Electronic Commerce and the Role of the WTO*, Special Study 2 (1998), www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf

Wortley, B. A., 'The Interaction of Public and Private International Law Today' (1954) 85 *Recueil des Cours* 239

Wrenn, Gregory J., 'Cyberspace Is Real, National Borders Are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace' (2002) 38 *Stanford Journal of International Law* 97

Wu, Tim, 'When Code Isn't Law' (2003) 89 *Virginia Law Review* 679

Wyngaert van den, Christine and Stessens, Guy, 'The International Non Bis in Idem Principle: Resolving Some of the Unanswered Questions' (1999) 48 *International and Comparative Law Quarterly* 779

Yahoo! Europe, *Comments on the Green Paper on a 'Rome 1 Regulation'* (2003), http://ec.europa.eu/justice_home/news/consulting_public/rome_i/news_summary_rome1_en.htm

Yntema, Hessel E., 'The Historic Bases of Private International Law' (1953) 2 *American Journal of Comparative Law* 297

Yum, Kyo Ho, 'The Interaction Between American and Foreign Libel Law: US Courts Refuse to Enforce English Libel Judgments' (2000) 49 *International and Comparative Law Quarterly* 132

Zander, Oliver, 'Recent Developments in German Internet Law' (October/November 2000) *Computer & Law* 36

Zittrain, Jonathan, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', in Adam Thierer and Clyde Wayne Crews Jr (eds.), *Who Rules the Net?* (Washington DC: Cato Institute, 2003), 13

Zittrain, Jonathan and Edelman, Benjamin, 'Documentation of Internet Filtering in Saudi Arabia' (2002), Berkman Center for Internet and Society, http://cyber.law.harvard.edu/home/

'Documentation of Internet Filtering Worldwide', in Organization for Security and Co-operation in Europe (OSCE) (Christiane Hardy and Christian Möller), *Spreading the Word on the Internet* (Vienna: OSCE, 2003)

INDEX

act of state doctrine, 206–7, 219
Ahlert, Christian, 281
aircraft, jurisdiction, 74
Akehurst, Michael, 211, 240, 243
Albrecht, A R, 249
Amazon, 68, 157, 161, 279, 281
American Bar Association, 83
Antigua and Barbuda, 104, 171–2, 179
arbitrariness, 72–3
arbitration, US Internet contracts, 66
auctions, 69, 146
Austin, John, 155, 156, 157, 204
Australia
  criminal jurisdiction
    effects doctrine, 95–6
    online security dealings, 97–8, 152
  defamation
    all destinations, 128–9, 254–5
    freely accessible sites, 127
    jurisdiction, 112, 288
    minimal access, 119–21
    targeted destinations, 137
  domain names, 269
  enforcement of foreign orders
    private/public dichotomy, 239, 241, 243
    public law orders, 222, 249
  gambling online, 173–4, 176, 193–6, 251
  hate speech, 108
  music copyright, 227
  spam, 258, 271, 277, 284
autonomy, 117, 182

Baade, Hans, 219, 250, 251
banking, diversity of laws, 264
Beech, Andrew, 113
Belgium, spam, 277, 284
Bell, Griffin, 224
belonging, 70, 74, 93
Bentham, Jeremy, 155
Berman, Paul Schiff, 259
blackmail, 165
blocking
  foreign illegal contents, 229–30, 283–7
borders
  See also geo-location technology
  borderless cyberspace, 117–19, 143
  country-specific sites, 13, 29, 281–2
  zoning solutions, 278–87
Bowrey, Kathy, 269
Brenner, Susan, 210, 263
Bruneau, Lynn, 61
Brussels Convention, consumer contracts, 75–6
Buxbaum, Hannah, 240, 244, 247
Byers, Michael, 44, 45

Canada
  criminal jurisdiction, Holocaust denial, 106–7
  defamation, 122
  enforcement of foreign law, 243
  hate speech, 108
  spam, cooperation, 258
Carter, P B, 241, 249
censorship, 285–6, 287
certainty
  arbitrariness and, 72–3
  harmonisation of competence rules, 260
  international law and, 88, 89
  jurisdiction, 94

rule of law and, 44
targeted destination approach and, 139–40
change
judicial reasoning, 43–5, 52
law as engine of change, 58–65
child protection
issues, 8
origin principle and, 182–3
UK gambling, 182–4
China, 29, 182, 279, 285
choice of forum
consumer exceptions, 69
contract, 66, 67
forum shopping, 178–81, 187
choice of law, contract, 21, 66, 67
choices
harmonisation. *See* harmonisation
hidden choice, 253–8
less transnational Internet, 278–87
value judgments, 287–90
circumvention methods, 281
civil law. *See* private international law
civil law systems, 43
Clinton, Bill, 57, 255
coding, 30–2, 278
comity, 211, 222, 224
common heritage of mankind, 20
common law systems, 43
communications, value, 290
company law jurisdiction, EU, 180
comparative law
approach, 6
jurisdictional approaches, 108–10
competition, 8
CompuServe, 102–3
concurrent jurisdictions, 21–2, 102–4
conflict of laws. *See* private international law
consequentialism, 45, 50
conservatism, jurisdiction decisions, 52–6
constructive presence, 90
consumer contracts
adjudicative jurisdiction, 74–9
European Union, 68, 114, 118, 280
unfair terms, UK, 67
consumer protection, 61–2, 68
contract
See also consumer contracts
choice of forum, 66, 67
consumer exceptions, 69
choice of law, 21, 66, 67
close connections, 67
electronic contracts, 264
freedom of contract, 66–9
Internet impact, 66–9
location factor, 67
standard form, 68
Cook Islands, 179
cooperation
extradition, 192, 201
future, 251–2, 253, 279
gambling online, 190–3
good neighbour clauses, 193–6, 251
international obligations, 191
moderate regulation and, 28
private law enforcement, 210–18
public policy exception, 214–18
public law non-cooperation, 218–30
lack of power or will, 221–5
taboo, 218–21
public/private dichotomy, 230–50
foreign states' involvement, 238
nature of remedies, 245–8
paradox, 248–50
public or private causes of action, 242–5
public or private complainants, 240–2
spectrum, 233–8
regulatory restraint and, 212
spam, 258
copyright
cyberspace protection, 64
music, 227
predictions, 61
quantitative impact of Web, 38
web links and, 36
Council of Europe, 217, 255, 263–4
country of destination. *See* destination principle
country of origin. *See* origin principle
country-specific sites. *See* borders
credit cards, 173

criminal jurisdiction
assessment of approaches, 109–10
civil v criminal, 70
common denominators, 102–8
concurrent jurisdictions, 102–4
diversity of values, 107–8
enforcement, 104–7
criminal law, 87–9
disclaimers, 152, 157, 161–2, 283
effects doctrine
crude effects doctrine, 94–6
reasonable effects doctrine, 91–4
evolution, 87–108
foreseeability of foreign law, 141–53
all destinations, 145–9
borderless cyberspace, 143
geo-location technology, 151
harm, 147
multiple interpretations, 141–3
reasonable foreseeability, 149–53
territoriality principle, 143–5
international crimes, 191–2
limits, 16–18
Lotus case, 89–91
mandatory character of law, 142, 161
objective territoriality principle, 25, 89
post-Internet developments, 96–102
Australian security dealings, 97–8, 152
Canadian Holocaust denial, 106–7
French Nazi memorabilia, 99–100, 105
German Holocaust denial, 100–1, 105
German obscenity laws, 102–3
UK pornography, 98–9, 105
US online gambling, 96–7, 102, 103, 104–5, 107
pre-Internet refinements, 89–96
public international law, 141
rules, 15
subjective territoriality principle, 25
substantive justice, 74
territoriality principle, 89, 141
Cuba, 182
cultural values
choices, 287–90
criminal jurisdiction, 107–8
customary international law
international crimes, 191–2
private law and, 211
role, 6
state practice and, 88, 89
uncertainty, 88
cyber-jurisdiction, 265–6
cybersquatting, 34

data protection, EU, 227, 276
defamation
adjudicative jurisdiction, 112–14
country of destination approach, 111–14, 138–41
cyberspace phenomenon, 111
dead persons, 160
deregulation, 266
foreseeability of foreign jurisdiction, 115–41
actual access, 119–25
all destinations, 127
borderless cyberspace, 117–19
destination principles, 138–41
foreign harm, 129–34
free sites, 125–38
subscription sites, 125–7
targeted destinations, 134–8, 150
mandatory law, 161
meaning of publication, 133–4
non-commercial online publications, 119
quantitative impact of Internet, 37
democracy
Internet force for, 4
values, 117
Denmark, 196
deregulation, 265–70
destination principle
advantages and disadvantages, 189–9
criminal jurisdiction, 145–9
defamation and, 111–14
disadvantages, 176
foreseeability, 111, 115
harmonisation by default, 271–5

moderate approach, 111, 137, 253
moderate v outright approach, 138–41
outright approach, 111
solution to jurisdiction issue, 24–6
targeting approach, 26
assessment, 138–41
defamation, 134–8
Scottish case law, 50
spam, 274–5
US, 48–9, 76–8, 82–7, 135–7, 147–9
zoning, 283–7
Dicey, A V, 211
disclaimers, 152, 157, 161–2, 283
dispute resolution, online, 267
Dodge, William S, 211
Doehring, Karl, 224
domain names
regulation, 268–70
trade marks and, 33–5, 65
US jurisdiction, 74
Dr Strangelove, 13
due process, 262

e-commerce
choice of forum, 69
contract law and, 66–9
disclaimers, 152, 157, 161–2, 283
European Union, 69, 184–9
small businesses, 68, 157, 160
e-mail, spam. *See* spam
eBay, 157, 267, 279
Edelman, Benjamin, 285, 286
Edwards, Lilian, 37
effects doctrine
crude effects doctrine, 94–6
reasonable effects doctrine, 91–4
US criminal jurisdiction, 147–9
egg story, 1–3, 12, 20, 24
Elz, Robert, 269
enforceability of foreign law
importance, 203–6, 207–10
motivations, 204
sanctions, 155–6, 203–4, 209
US Yahoo litigation, 202–3, 205–6
enforcement of foreign law
See also Yahoo litigation
criminal jurisdiction and, 104–7
enforceability v enforcement, 203–6
exemplary damages, 246–7
extra-territorial jurisdiction, 222
future, 251–2
gambling laws, US, 104–5, 107, 173, 176
jurisdiction, 18
limited powers, 26–8, 199–203
private law cooperation, 210–18
public policy exceptions, 214–18
public law non-cooperation, 218–30
lack of power or will, 221–5
public law taboo, 218–21
public/private dichotomy
cooperation and, 230–50
foreign state interests, 238
nature of remedies, 245–8
paradox, 248–50
public or private causes of action, 242–5
public or private complainants, 240–2
spectrum, 233–8
territoriality principle, 200
unilateral strategies, 225–30
analogous local prohibitions, 227
blocking illegal contents, 229–30, 283–7
penalisation of intermediaries, 173, 226
prohibition of local supportive services, 228–9
symbolic prosecutions, 225–6
voluntary compliance, 206–7
environmental responsibility, 191
European Union
blocking and, 286
consumer contracts, 76–8, 114, 280
consumer protection, 68
data protection, 227, 276
defamation, 124–5
e-commerce, 69, 184–9
liability of intermediaries, 228
free movement principle, 185
gambling online, 168–9
harmonisation of laws, 187, 188
junk-mail, 258
jurisdiction
company law, 180

European Union (*cont.*)
damage-focused approach, 131
directing test, 86–7, 118
regulation, 67
Rome II, 131
mutual recognition, 185, 186, 188
political integration, 250
Safer Internet Programme, 267
Services Directive, 186
single market, 185
spam, 57, 275–7
Television without Frontiers Directive, 186, 188
exemplary damages, 246–7
Expedia, 279, 281
extra-territorial jurisdiction, 222
extradition, 192, 201

federations, 15
Feld, Harold, 269
Ferguson, Niall, 250
filtering, 174, 267, 284
financial services
Australian securities dealings, 97–8, 152
diversity of laws, 264
zoning, 282
floodgate argument, 59–62, 64
foreign law
borderless cyberspace, 117–19
commercial attitudes, 207–10
country of destination. *See* destination principle
country of origin. *See* origin principle
defamation. *See* defamation
enforceability. *See* enforceability of foreign law
enforcement. *See* enforcement of foreign law
foreseeability of criminal law, 141–53
legitimacy, 205, 206, 208–10
notice, 111–15
actual notice, 153–7
traditional methods of publication, 157–9
foreseeability
destination approach, 111, 115
foreign criminal jurisdiction, 141–53
all destinations, 145–9
borderless cyberspace, 143
multiple interpretations, 141–3
reasonable foreseeability, 149–53
territoriality principle, 143–5
foreign defamation jurisdiction, 115–41
actual access, 119–25
all destinations, 127
borderless cyberspace, 117–19
destination principles, 138–41
foreign harm, 129–34
free sites, 125–38
targeted destinations, 134–8, 150
origin approach, 164
rule of law, 115–17, 125
forum non conveniens, 21
forum shopping, 178–81, 187
France
See also Yahoo litigation (France)
collective memory of WWII, 233
country-specific Google site, 29
criminal jurisdiction
enforcement, 105
notice of law, 160–1
Google site, 279
hate speech, 108, 201–3
language purity laws, 203
mopeds, 271
prohibition of nazi memorabilia, 209, 227
territorial restrictions techniques and, 103
freedom of contract, 66–9
freedom of expression, 103, 150, 207, 264–5
Fuller, Lon, 290
futility argument, 62–4

gambling online
See also specific countries
diversity of laws, 27, 264
foreign providers' local activities, 167–75
rejection of origin principle, 167–75

UK adoption of origin principle, 175–84
WTO/GATS, 171–3
local providers' foreign activities, 190–6
good neighbour clauses, 193–6, 251
lack of cooperation, 190–3
UK and Australia, 193–6, 251
online v national location, 8
origin principle, paradigm, 166–7
UK adoption of origin principle, 175–84
child protection, 182–4
economic argument, 176–8
forum shopping, 178–81
Gambling Act 2005, 175–6
lowest common denominator, 184
model, 197–8
no protection from foreign harm, 182–4
race to the bottom, 178–81
shift of regulatory burden, 181
Garnett, Richard, 259
GATS, 171–3
geo-location technology
circumvention, 281
concurrent jurisdictions and, 104
criminal jurisdiction and, 63, 151
France, 103
spam and, 273
zoning, 278, 281–2
Germany
adjudicative jurisdiction, 50
cooperation, public law, 224
criminal jurisdiction
Holocaust denial, 100–1, 105, 147
obscenity laws, 102–3
online Nazi memorabilia, 99–100
gambling online, 167–8, 169
Google site, 29, 279
hate speech, 108
judicial activism, 43
pharmaceuticals, 186
value judgments, 288
Gladwell, Malcolm, 70
global law. *See* harmonisation
'global village', 4
Goodman, Marc, 210, 263
Google, 29, 157, 173, 199, 279, 285
Grabosky, P N, 265
Graveson. R H, 211
Grenada, 179

Hague Conference on Private International Law, 7, 259
harmonisation
by default, 270–7
destination approach, 271–5
origin approach, 275–7
by design, 262–70
deregulation, 265–70
treaties, 263–5
competence rules, 259–62
cooperation and, 251–2
desirability, 256
European Union, 187, 188
more global law, 258–9
spam, 257
v territoriality principle, 28–30
Hart, H L A, 155–6, 204, 209
Harvey, Fiona, 257
hate speech, 107, 199, 263, 273
See also Yahoo litigation
Hestermeyer, Holger, 259
Holder, William, 220
Holocaust denial
Canada, 106–7
Germany, 100–1, 105, 147
human dignity, 117, 143

ICANN, 65, 268–70
in rem jurisdiction, 70, 74
indirect regulation, 154
intellectual property, 54
See also copyright; trade marks
intermediaries, penalisation, 173, 226
international criminal law, 191–2
international law
See also private international law; public international law
certainty and, 88, 89
environmental responsibility, 191
legal reasoning, 42
non-intervention principle, 191, 200

international law (*cont.*)
public/private law dichotomy, 231–3
International Telecommunications Union, 257, 277
Internet
Global Net v national laws, 1–13
impact on law, 35–40
contract law, 66–9
new qualitative problems, 35–6, 37
new quantitative problems, 37–9
severity of problems, 39–40
meaning, 3
ubiquity, 39–40
unruliness, 199–203
Internet Service Providers, filtering, 174
Ireland, 241
Italy, 122, 168, 176–7, 227

Jennings, Robert, 88, 141
Johnson, David R, 11–12, 33, 34, 47, 51, 56–7, 59, 60, 62, 63, 117–18, 143, 265
judicial reasoning
activism, 43
best v least disruptive solutions, 56–8
consequentialism, 45, 50
conservatism, 52–6
consistency, 45
continuity and change, 43–5, 52
creativity, 53
floodgate argument, 59–62, 64
futility argument, 62–4
risk management strategies, 60
websites as basis of jurisdiction, 47–52
junk-mail, 258
jurisdiction
assessment of approaches, 108–10
belonging, 70, 74, 93
best v least disruptive solutions, 56–8
civil v criminal law, 70
concept, 13–15
concurrent jurisdictions, 21–2, 102–4
conservatism, 52–6
criminal law, 87–9
cyber-jurisdiction, 265–6
defamation. *See* defamation
definition, 13–18
European Union, 67
harmonisation, 259–62
judicial reasoning, 47–58
links, 20–4
location, 20–1
nationality principle, 20–1
prescription/adjudication/enforcement, 16–18
private law. *See* private international law
public law. *See* criminal jurisdiction
rules, 15–18
solutions, 24–32
country of destination. *See* destination principle
country of origin. *See* origin principle
harmonisation. *See* harmonisation
limited enforcement jurisdictions, 26–8
technical regulation, 30–2, 278
territoriality v harmonisation, 28–30
zoning, 278–87
substantive v formal justice, 71–4
territoriality principle. *See* territoriality principle
universal jurisdiction, 21, 22, 192
websites as basis of jurisdiction, 47–52, 54, 59
justice
substantive justice, 78
substantive v formal, 71–4

Kaiser, Karl, 10
Kelsen, Hans, 153, 155, 156, 204, 231, 238, 241
Koogle, Timothy, 100, 160, 244
Korea, 258
Kramer, Larry, 150

Lainos, Michalis, 158
Lauterbach, H, 236
law

change
judicial reasoning, 43–5, 52
legislation, 45–6
tipping point, 69–74
efficacy, 153–7, 204
engine of change, 58–65
cautious way forward, 64–5
floodgate argument, 59–62, 64
futility argument, 62–4
foreign law. *See* foreign law
indirect regulation, 154, 174
Internet impact on, 35–40
new qualitative problems, 35–6
new quantitative problems, 37–9, 59–62
severity of problems, 39–40
legal doctrines
building blocks, 13–24
jurisdiction. *See* jurisdiction
role, 12
legitimacy, 209
methods of publication
online failures, 159–62
traditional methods, 157–9
sanctions, 155–6, 203–4, 209
tipping point, 69–74
evolution of law v tipping point, 69–71
substantive v formal justice, 71–4
Ledig, Robert, 61
legal reasoning
jurisdictional challenge, 47–58
process, 41–3
legislation. *See* regulation
Lenin, 238
Lessig, Lawrence, 30, 63, 64, 154, 156, 194–5, 251, 278
lex mercatoria, 40
liberalism, 31–2, 255–6, 278–87
LICRA, 202
links, copyright and, 36
lis alibi pendens, 21
Lombois, Claude, 200, 251
Lowenfeld, Andreas, 93, 218, 236
Luban, David, 158

McConnaughay, Philip, 95, 142, 220
MacCormick, Neil, 44, 60, 72, 289–90
McIntosh, Lord, 196
McLuhan, Marshall, 4
Maggs, Peter, 266, 267
Malaysia, defamation, 122
Mann, F A, 9, 18, 82, 93–4, 212, 220, 223, 231, 235
Mann, Michael, 246
Marks & Spencer's, 161, 282
Meng, Werner, 223
Merryman, John Henry, 231, 232
Milgram, Stanley, 156
moral values
choices and, 287–90
criminal jurisdiction and, 107–8
Yahoo litigation, 203
music copyright, 227

national regulation of Global Net
building blocks, 13–24
conservative approach, 11–13
diversity, 27
egg story, 1–3, 12, 20, 24
generally, 1–13
irreconcilability, 253–8
jurisdiction. *See* jurisdiction
legal landscape, 3–6
relevance, 6–11
solutions, 24–32
country of destination. *See* destination principle
country of origin. *See* origin principle
global law. *See* harmonisation
hidden choice, 253–8
limited enforcement jurisdictions, 26–8
technical regulation, 30–2
territoriality v harmonisation, 28–30
value judgments, 287–90
zoning, 278–87
nationality, jurisdiction and, 20–1
Nazi memorabilia. *See* Yahoo litigation
negligence, car accidents, 73–4
Netherlands, 167–8, 271
netiquette, 265
New Zealand, 174, 237, 285
non-intervention principle, 191

notice of law
foreign law, 111–15
actual notice, 153–7
borderless cyberspace, 117–19
publication methods
online failures, 159–62
traditional methods, 157–9
nulla poena sine culpa, 226

obscenity, 102–3
OECD, 6, 257
opinio juris, 6, 42
Oren, Joakim, 114, 157, 162, 280
origin principle
advantages and disadvantages, 189–9
E-Commerce Directive and, 184–9
economic losses, 176–8, 187
exclusive approach, 164–7
forum shopping, 178–81, 187
gambling online, 166–7
rejection of principle, 167–75
UK adoption of principle, 175–84
harmonisation by default, 275–7
lowest common denominator, 184
meaning, 166
no protection from foreign harm, 182–4
race to the bottom, 178–81
shift of regulatory burden, 181
solution to jurisdiction issue, 24–6
territoriality principle, 165
zoning, 278–83

paternalism, 182
Pfizer, 282
pharmaceuticals, 166, 182, 186, 282
pornography
diversity of national laws, 27
enforcement issues, 199
penalising local consumers, 227
UK jurisdiction, 98–9, 105, 145–6
US regulation, 63, 64, 286
positivism, 204
Post, David, 11–12, 33, 34, 47, 51, 56–7, 59, 60, 62, 63, 117–18, 143, 265
Postel, Jon, 269
private international law
assessment of approaches, 108, 109
concept of jurisdiction, 14
consumer contracts, 74–9
evolution, 74–87
Internet refinements, 82–7
jurisdictional links, 23
meaning of private law, 19
pre-Internet refinements, 79–82
public/private dichotomy, 15–16, 19, 70, 231–3
foreign state involvement, 238
nature of causes of action, 242–5
nature of remedies, 245–8
paradox, 248–50
public or private complainants, 240–2
spectrum, 233–8
See also Yahoo litigation
terminology, 17
protectionism, 171
Pryles, Michael, 113
public international law
See also criminal jurisdiction
cooperation, 201
criminal jurisdiction, 141
meaning, 19
objectives, 142
private law v, 19
public/private dichotomy, 231–3
foreign state interests, 238
foreign state involvement, 240–2
nature of remedies, 245–8
paradox, 248–50
public or private causes of action, 242–5
spectrum, 233–8
See also Yahoo litigation
territorial jurisdiction, 25
public law jurisdiction. *See* criminal jurisdiction
public morality exceptions, WTO, 172
public policy
enforcement of foreign orders, 206, 209, 214–18
non-cooperation policy, 237
publication

meaning, 133–4
publication of law
online failures, 159–62
traditional methods, 157–9
punitive damages, 246–7

race to the bottom, 178–81
Raw, Hazel, 274
Raz, Joseph, 116, 153, 157
Reagan, Ronald, 154
reasoning
judicial reasoning, 43–5
legal reasoning, 41–3
regulation
cautious way forward, 64–5
change and continuity, 45–6
cooperation and regulatory restraint, 212
indirect regulation, 154, 174
least disruptive solutions, 57–8
Reidenberg, Joel, 57, 280, 284
Rice, Denis T, 285
road traffic accidents, negligence, 73–4
Roman law, 14
rule of law
certainty, 44
foreseeability and, 115–17, 125

Safer Internet Programme, 267
sanctions, 155–6, 203–4, 209
Saudi Arabia, 285
Scotland, trade mark jurisdiction, 50, 137–8
securities trading, 97–8, 152, 264
self-government of cyberspace, 11, 265–70
ships, jurisdiction, 74
Show/Time, 280, 281, 283
Singapore, 285
sliding scale test, 83–6
small businesses, 68, 157, 160
Smith, Graham J H, 285
Smith, Russell G, 265
solutions, hidden choice, 253–8
sovereignty principle, 9, 191, 200
spam
costs, 257
EU regulation, 57, 275–7
filters, 284
harmonisation of regulation by default
destination principle, 271–5
origin approach, 275–7
lack of harmonisation, 257
limited enforcement powers, 199
regulation paradigm, 257–8
technological measures, 258
zoning option, 280
stare decisis, 41, 44, 65
states
federations, 15
sovereignty, 9, 191, 200
state practice, 6–11, 42, 88, 89
territoriality principle, 8–9
viability, 9–11
Stein, Allan, 81
Steinberger, Helmut, 250
Stoel, Thomas, 220, 223
Svantesson, Dan Jerket, 273, 280, 281

taxation, 36, 38
technical processes
See also geo-location technology
impact on law, 35
legal reasoning and, 41, 52
relevance to law, 13
spam regulation, 258
territoriality principle
See also borders
contract, 67
country of origin approach, 165
country of origin/destination, 24–6
criminal jurisdiction, 89, 141
constructive presence, 90
crude effects doctrine, 94–6
foreseeability, 143–5
objective territoriality principle, 89
online Holocaust denial, 101
reasonable effects doctrine, 91–4
enforcement, 200
v harmonisation, 28–30
jurisdictional rule, 8–9, 14, 20–1
post-Internet issues, 110
private law, 74–5
torts, 25
terrorism, 286

Thailand, 258
tipping point, 69–74
Torres Bernardez, Santiago, 143
torts, 25
trade marks
  domain names and, 33–5, 65
  legal assumptions, 37
  Scottish case law, 50, 137–8
  US case law, 48
transfer pricing, taxation, 38
treaties, harmonisation through, 263–5

UEJF, 202
UNCITRAL, 263
Unger, Roberto, 12
unilateralism
  analogous local prohibitions, 227
  blocking illegal contents, 229–30, 283–7
  penalisation of intermediaries, 226
  prohibition of local supportive services, 228–9
  strategies, 225–30
  symbolic prosecutions, 225–6
United Arab Emirates, 285
United Kingdom
  adjudicative jurisdiction, 18, 50
  criminal jurisdiction
    enforcement, 105
    online pornography, 98–9, 105, 145–6
  defamation
    all destinations, 127–8
    dead persons, 160
    foreign harm, 129–30, 133–4
    freely accessible sites, 125–6
    jurisdiction, 112
    minimal access, 121–2, 123
  enforcement of foreign law, 243
    exemplary damages, 246
    public law, 222, 224
    public policy exceptions, 214
  firearms regulation, 158
  gambling law, 271
    adoption of origin principle, 166–7, 175–84
    child protection, 182–4
    economic argument, 176–8
    forum shopping, 178–81
    Gambling Act 2005, 175–6
    good neighbour clauses, 193–6, 251
    lowest common denominator, 184
    model, 197–8
    no protection from foreign harm, 182–4
    race to the bottom, 178–81
    shift of regulatory burden, 181
  music copyright, 227
  service out of jurisdiction, 75
  spam, cooperation, 258
  unfair terms in consumer contracts, 67
  value judgments, 288
United States
  abortions, 154
  adjudicative jurisdiction, 18, 52
  arbitration clauses, 66
  civil jurisdiction, 118
    Internet refinements, 82–7
    pre-Internet refinements, 79–82
    sliding scale test, 83–6
    targeting test, 48–9, 77, 78, 82–3
  criminal jurisdiction
    Alcoa case, 144–5
    antitrust laws, 142, 144
    crude effects doctrine, 94–6
    effects doctrine, 147–9
    extension, 142, 144–5
    reasonable effects doctrine, 91–3
  defamation
    Constitutional obstacles, 112
    public figure doctrine, 130, 160
    single publication rule, 123–4
    targeted destinations, 135–7
  destination approach, 147–9
  domain names jurisdiction, 74
  enforcement of foreign orders
    due process, 262
    private law, 210
    public law, 218, 221–2
    public/private dichotomy, 245
    See also Yahoo litigation (US)
  exemplary damages, 246
  firearms regulation, 162

freedom of expression, 103, 207
gambling online
criminal jurisdiction, 96–7, 102, 103, 104–5, 107
enforcement, 104–5, 107, 173, 176
intermediaries, 173, 285
national economic interest, 171
rejection of origin principle, 169–71
WTO dispute, 171–2
hate speech, 107
Internet jurisdiction literature, 6
music copyright, 227
pornography regulation, 63, 64, 228, 286
protectionism, 171
public policy, 206, 209
spam, 258, 266, 272, 277
territoriality principle, 81
trade marks case law, 48
withdrawal from Internet administration, 11
Yahoo. *See* Yahoo litigation (US)
universal jurisdiction, 21, 22, 192

value judgments, 287–90
Vartanian, Thomas, 61
Venezuela, 179
vicarious liability, 226
viruses, 257
vulnerable groups, 182

Watts, Arthur, 88, 141
weapons, 182, 199
Wittgenstein, Ludwig, 290
World Summit on the Information Society, 5
WTO
gambling online, 171–3
Internet jurisdiction literature, 7
public morality exceptions, 172

Yahoo, 173, 273, 279
Yahoo litigation (France)
criminal jurisdiction, 99–100, 146–7, 202, 213, 280
foreseeability, 146–7
objective of litigation, 160
outline, 201–3
public or private law, 203, 218, 233–5, 245
Yahoo French subsidiary, 105, 226
Yahoo litigation (US)
act of state doctrine, 206–7, 219
enforceability issue, 205–6, 207–10
outline, 202–3
private law cooperation, 210
public policy exception, 206, 209, 214–18
private or public case, 233–5
foreign state's interest, 239–40
nature of cause of action, 244
paradox, 249
private litigants, 242
remedy, 247–8
voluntary compliance, 206–7

Zittrain, Jonathan, 285, 286
zoning solutions
coding, 30–2, 278
countries of destination, 283–7
countries of origin, 278–83
generally, 278–87