The Liability of Internet Intermediaries

Jaani Riordan

Magdalen College, Oxford

Thesis submitted for the degree of
Doctor of Philosophy in Law

Hilary Term, 2013

Word Count: 101 200

Abstract

[Internet intermediaries facilitate a wide range of conduct using services supplied over the layered architecture of modern communications networks. Members of this class include search engines, social networks, internet service providers, website operators, hosts, and payment gateways, which together exert a critical and growing influence upon national and global economies, governments and cultures. This research examines who should face legal responsibility when wrongdoers utilise these services tortiously to cause harm to others. It has three parts.

Part 1 seeks to understand the nature of an intermediary and how its liability differs from the liability of primary defendants. It classifies intermediaries according to a new layered, functional taxonomy and argues that many instances of secondary liability in English private law reflect shared features and underlying policies, including optimal loss-avoidance and derivative liability premised on an assumption of responsibility.

Part 2 analyses intermediaries' monetary liability for secondary wrongdoing in two areas of English law: defamation and copyright. It traces the historical evolution of these doctrines at successive junctures in communications technology, before identifying and defending limits on that liability which derive from three main sources: (i) in-built limits contained in definitions of secondary wrongdoing; (ii) European safe harbours and general limits on remedies; and (iii) statutory defences and exceptions.

Part 3 examines intermediaries' non-monetary liability, in particular their obligations to disclose information about alleged primary wrongdoers and to cease facilitating wrongdoing where it is necessary and proportionate to do so. It proposes a new suite of non-facilitation remedies designed to restrict access to tortious internet materials, remove such materials from search engines, and reduce the profitability of wrongdoing. It concludes with several recommendations to improve the effectiveness and proportionality of remedies by reference to considerations of architecture, anonymity, efficient procedures, and fundamental rights.]

Table of contents

Chapter 2: The Nature of an Intermediary

Chapter 3: The Concept of Secondary Liability

PART 2 — MONETARY LIABILITY

Chapter 4: Defamation

Chapter 5: Copyright

Chapter 7: Non-facilitation

Chapter 8: Conclusion

Table of abbreviations

1911 Act	*Copyright Act 1911* (Imp)
1996 Act	*Defamation Act 1996* (UK)
2012 Bill	Defamation Bill 2012 (UK)
2LD	second-level domain (eg, `http://google.co.uk/`)
A&M Records	*A & M Records Inc v Audio Magnetics Incorporated (UK) Ltd* [1979] FSR 1
ACTA	*Anti-Counterfeiting Trade Agreement*
ADR	alternative dispute resolution
Amazon	*McGrath v Dawkins* [2012] EWHC B3 (QB)
Ames	*CBS Inc v Ames Records & Tapes Ltd* [1982] Ch 91
Amstrad v BPI	*Amstrad Consumer Electronics plc v The British Phonographic Industry Ltd* [1986] FSR 159
Anton Piller	*Anton Piller KG v Manufacturing Processes* [1976] Ch 55
API	application programming interface
Ash	*Ash v Hutchinson and Co (Publishers) Ltd* [1936] 1 Ch 489
Ashworth	*Ashworth Hospital Authority v MGN Ltd* [2002] 1 WLR 2033
BAE	*Campaign against Arms Trade v BAE Systems plc* [2007] EWHC 330 (QB)
Barclays Bank	*Customs and Excise Commissioners v Barclays Bank plc* [2007] 1 AC 181
Belegging	*Belegging-en Exploitatie Maatschappij Lavender BV v Witten Industrial Diamonds Ltd* [1979] FSR 59
BERR	Department for Business, Enterprise and Regulatory Reform
BIS	Department for Business, Innovation and Skills
BMG Canada	*BMG Canada Inc v John Doe* (2005) 252 DLR (4th) 342
British Steel	*British Steel Corporation v Granada Television Ltd* [1981] AC 1096
BT	*R (British Telecommunications plc) v Secretary of State* [2011] EWHC 1021 (Admin)
BT (CA)	*R (British Telecommunications plc) v Secretary of State* [2012] EWCA Civ 232
Byrne	*Byrne v Deane* [1937] 1 KB 818
C Inc v L	*C Inc plc v L* [2001] 2 Lloyd's Rep 459
Cadbury	*Cadbury Ltd v Ulmer GmbH* [1988] FSR 385
Campbell	*Campbell v MGN Ltd* [2004] 2 AC 457
Cardile	*Cardile v LED Builders Pty Ltd* (1999) 198 CLR 380
CBS	*CBS Songs Ltd v Amstrad Consumer Electronics plc* [1988] 1 AC 1013

Chabra	*TSB Private Bank International SA v Chabra* [1992] 1 WLR 231
Channel Tunnel	*Channel Tunnel Group Ltd v Balfour Beatty Construction Ltd* [1993] AC 334
Charter	*Charter of Fundamental Rights and Freedoms of the European Union*
Ciryl	*Performing Right Society Ltd v Ciryl Theatrical Syndicate Ltd* [1924] 1 KB 1
CJEU	Court of Justice of the European Union
Clift	*Clift v Clarke* [2011] EWHC 1164 (QB)
Coca-Cola	*Coca-Cola Company v British Telecommunications plc* [1999] FSR 518
Code	OFCOM, *Online Copyright Infringement Initial Obligations Code* (2010)
Communications Act	*Communications Act 2003* (UK)
Convention	*European Convention for the Protection of Human Rights and Fundamental Freedoms*
Cooper	*Universal Music Australia Pty Ltd v Cooper* (2005) 150 FCR 1
Copyright Act	*Copyright, Designs and Patents Act 1988* (UK)
Creative Britain	Department for Culture, Media and Sport, *Creative Britain: New Talents for the New Economy* (2006)
Credit Lyonnais	*Credit Lyonnais Bank Nederland NV v Export Credits Guarantee Department* [2000] 1 AC 486
Data Retention Directive	Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2006] OJ L 105/54
Data Retention Regulations	*Data Retention (EC Directive) Regulations 2009* (UK)
Davison	*Davison v Habeeb* [2011] EWHC 3031 (QB)
DEA	*Digital Economy Act 2010* (UK)
Defamation and the Internet	Matthew Collins, *The Law of Defamation and the Internet* (2nd ed, 2005)
DMCA	*Digital Millennium Copyright Act 1998* (US)
DNS	Domain Name System
Dorset Yacht	*Dorset Yacht Co Ltd v Home Office* [1970] AC 1004
DPA	*Data Protection Act 1998* (UK)
DPI	deep packet inspection
Dramatico	*Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch)
Dramatico [No 2]	*Dramatico Entertainment Ltd v British Sky Broadcasting Ltd [No 2]* [2012] EWHC 1152 (Ch)
eBay	*L'Oréal SA v eBay International AG* [2009] RPC 21
eBay (CJEU)	Case C-324/09, *L'Oréal SA v eBay International AG* [2011] ETMR 52

E-Commerce Directive	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market [2000] OJ L 178/1
E-Commerce Regulations	*Electronic Commerce (EC Directive) Regulations 2002* (UK)
Emmens	*Emmens v Pottle* (1885) QBD 354
Enforcement Directive	Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights [2004] OJ L 157/45
EU	European Union
Falcon	*Falcon v The Famous Players Film Co Ltd* [1926] 2 KB 474
Fourie	*Fourie v Le Roux* [2007] 1 WLR 320
Framework Directive	Directive 2009/140/EC [2009] OJ L 337/37
French Civil Code	*Code Civil* (France) (*Version consolidée au 1 janvier 2013*)
Gatley on Libel and Slander	Patrick Milmo et al (eds), *Gatley on Libel and Slander* (11th ed, 2010)
Godfrey	*Godfrey v Demon Internet Ltd* [2001] QB 201
Golden Eye	*Golden Eye (International) Ltd v Telefónica UK Ltd* [2012] EWHC 723 (Ch)
Goldsmith	*Goldsmith v Sperrings Ltd* [1977] 1 WLR 478
Google France	Joined Cases C-236/08, C-237/08 and C-238/08, *Google France Sarl v Louis Vuitton Malletier SA* [2010] RPC 19
Gowers Review	Andrew Gowers, *Gowers Review of Intellectual Property* (December 2006)
Hays	*Hays plc v Hartley Ltd* [2012] EWHC 1068 (QB)
Home Office Voluntary Code	Home Office, *Retention of Communications Data under Part 11: Anti-terrorism, Crime & Security Act 2001: Voluntary Code of Practice* (2001)
HRA	*Human Rights Act 1998* (UK)
ICANN	Internet Corporation for Assigned Names and Numbers
IFPI	International Federation of the Phonographic Industry
iiNet	*Roadshow Films Pty Ltd v iiNet Ltd [No 3]* [2010] FCA 24
iiNet (Full Court)	*Roadshow Films Pty Ltd v iiNet Ltd* [2011] FCAFC 23
iiNet (HCA)	*Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16
Information Society Directive	Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10
Interbrew	*Interbrew SA v Financial Times Ltd* [2002] EMLR 24
Intercen	*Morton–Norwich Products Inc v Intercen Ltd* [1978] RPC 501

Interflora	*Interflora Inc v Marks and Spencer plc* [2009] RPC 22
IP	Internet Protocol
IPO	Intellectual Property Office
ISP	internet service provider
Jade Engineering	*Jade Engineering (Coventry) Ltd v Antiference Window Systems Ltd* [1996] FSR 461
Jameel	*Jameel v Dow Jones & Co Inc* [2005] QB 946
John Walker	*John Walker & Sons Ltd v Henry Ost & Co Ltd* [1970] 1 WLR 917
Karno	*Karno v Pathé Frères* (1909) 100 LT 260
Kaschke	*Kaschke v Gray* [2010] EWHC 690 (QB)
Lyon	*Lyon v Knowles* (1863) 3 B & S 556; 122 ER 209
Mareva	*Mareva Compania Naviera SA v International Bulkcarriers SA* [1975] 2 Lloyd's Rep 509
Marleasing	Case C-106/89, *Marleasing SA v La Comercial Internacional de Alimentación SA* [1990] ECR I-4135
MCA Records	*MCA Records Inc v Charly Records Ltd* [2002] FSR 26
McLeod	*McLeod v St Aubyn* [1899] AC 549
Media CAT	*Media CAT Ltd v Adams* [2011] FSR 28
Media CAT [No 2]	*Media CAT Ltd v Adams [No 2]* [2011] FSR 29
Mercedez-Benz	*Mercedez-Benz AG v Leiduck* [1996] AC 284
Metropolitan	*Metropolitan International Schools Ltd v DesignTechnica Corp* [2009] EWHC 1765 (QB)
Mitchell	*Performing Right Society Ltd v Mitchell and Booker (Palais de Danse) Ltd* [1924] 1 KB 762
Mitsui	*Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] EWHC 625 (Ch)
Mobilisa	*Mobilisa Inc v Doe 1*, 170 P 3d 712 (Ariz Ct App, 2007)
Mohamed	*R (on the application of Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2009] 1 WLR 2579
Newsquest	*Karim v Newsquest Media Group Ltd* [2009] EWHC 3205 (QB)
Newzbin	*Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] FSR 21
Newzbin2	*Twentieth Century Fox Film Corporation v British Telecommunications plc* [2011] EWHC 1981 (Ch)
Newzbin2 Order	*Twentieth Century Fox Film Corporation v British Telecommunications plc* [2011] EWHC 2714 (Ch)
Nikitin	*Nikitin v Richards Butler LLP* [2007] EWHC 173 (QB)
Norwich Pharmacal	*Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133
OBG	*OBG Ltd v Allan* [2008] 1 AC 1
Ocular Sciences	*Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289

OECD	Organisation for Economic Co-operation and Development
OFCOM	Office of Communications
One in a Million	*British Telecommunications plc v One In A Million Ltd* [1999] 1 WLR 903
OSI	Open Systems Interconnection
P v T	*P v T Ltd* [1997] 1 WLR 1309
P2P	peer-to-peer
Parbulk II	*Parbulk II AS v PT Humpuss Intermoda Transportasi TBK* [2011] 2 CLC 988
Paterson Zochonis	*Paterson Zochonis Ltd v Marfarken Packaging Ltd* [1983] FSR 273
PEC Directive	Directive 2002/58/EC on privacy and electronic communications [2002] OJ L 201/37
Plato	*Microsoft Corporation v Plato Technology Ltd* [1999] FSR 834
Promusicae	Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271
QC Leisure	*Football Association Premier League Ltd v QC Leisure* [2008] FSR 789
QoS	Quality of Service
Redland Bricks	*Redland Bricks Ltd v Morris* [1970] AC 652
Royal Brunei	*Royal Brunei Airlines Sdn Bhd v Tan* [1995] 2 AC 378
Sabaf	*Sabaf SpA v Meneghetti SpA* [2003] RPC 264
Sheffield	*Sheffield Wednesday Football Club Ltd v Hargreaves* [2007] EWHC 2375 (QB)
Scarlet	Case C-70/10, *Scarlet Extended SA v Société des Auteurs, Compositeurs et Éditeurs SCRL* [2011] ECR-I 0000
Searose	*Searose Ltd v Seatrain (UK) Ltd* [1981] 1 WLR 894
SEO	search engine optimisation
Siskina	*Siskina (Owners of Cargo Lately Laden on Board) v Distos Compania Naviera SA* [1979] AC 210
Sky	*Twentieth Century Fox Film Corporation v British Sky Broadcasting Ltd* (Unreported, 12 December 2011, Vos J)
Sportradar	*Football Dataco Ltd v Sportradar GmbH* [2012] EWHC 1185 (Ch)
TalkTalk	*Twentieth Century Fox Film Corporation v TalkTalk Telecom Group plc* (Unreported, 9 February 2012, Arnold J)
Tamiz	*Tamiz v Google Inc* [2012] EWHC 449 (QB)
Tamiz (CA)	*Tamiz v Google Inc* [2013] EWCA Civ 68
TCP/IP	Transmission Control Protocol/Internet Protocol
Technical Standards Directive	Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L 217/18

Tele2	Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-1227
TFEU	*Treaty on the Functioning of the European Union*
The Koursk	*The Koursk* [1924] P 140
Tilley	*Bunt v Tilley* [2007] 1 WLR 1243
TLD	top-level domain (eg, `http://google.com/`)
Total	*Revenue and Customs Commissioners v Total Network SL* [2008] 1 AC 1174
Totalise	*Totalise plc v The Motley Fool Ltd* [2002] 1 WLR 1233
TPB	The Pirate Bay
TRIPS Agreement	*Agreement on Trade-Related Aspects of Intellectual Property Rights*
UDRP	Internet Corporation for Assigned Names and Numbers, *Uniform Domain-Name Dispute-Resolution Policy* (approved 24 October 1999)
Unilever	*Unilever plc v Gillette (UK) Ltd* [1989] RPC 584
URL	Uniform Resource Locator
VeRO	Verified Rights Owner
Viagogo	*Rugby Football Union v Viagogo Ltd* [2011] EWHC 764 (QB)
Viagogo (CA)	*Rugby Football Union v Viagogo Ltd* [2011] EWCA Civ 1585
Viagogo (SC)	*Rugby Football Union v Consolidated Services Ltd (formerly Viagogo Ltd) (in liq)* [2012] 1 WLR 3333
WEA	*WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274
White Book	Lord Justice Jackson (ed), *The White Book* (2013 ed)
Wikimedia	*G v Wikimedia Foundation Inc* [2010] EMLR 14
WIPO	World Intellectual Property Organization

Table of cases

United Kingdom

European Union

Australia

United States of America

Other jurisdictions

Table of statutes

United Kingdom

European Union

Australia

United States of America

Other jurisdictions

International treaties

Table of other primary legal sources

Table of diagrams and tables

Acknowledgements

I am very grateful to my supervisor, Professor Roderick Bagshaw, for his insightful comments and generosity of time throughout this project.

The helpful and detailed comments of my transfer and confirmation assessors have also been invaluable in refining the scope and direction of this research, and in particular chapters 4 and 6.

I am grateful to my parents, family and friends for their ideas and support, and in particular to Mr Eli Ball, Mr Andrew Coffey, Mr Benedict Coxon, Mr Quentin Cregan and Mr Benjamin Spagnolo for our fruitful discussions. Any errors are, of course, my own.

I also acknowledge the assistance of the Clarendon Fund and James Fairfax Oxford–Australia Trust, without which this research would not have been possible.

This research reflects the law as it stood at 1 March 2013. Unless otherwise stated, all referenced website materials were last accessed on that date.

Jaani Riordan

April 2013

1
Introduction

Internet intermediaries occupy a central role in modern commerce, social and political life, and the dissemination of ideas. They are the conduits through which all electronic transmissions pass, custodians of our data and gatekeepers of the world's knowledge. This research has two objectives. First, it seeks to analyse and map the legal rules governing these parties' secondary liability for third parties who commit wrongdoing using their services. More generally, it identifies the principles which determine *who* should be liable for civil wrongdoing on the internet and *how* private rights should be enforced online. It does so by examining the secondary liability rules applicable to two civil wrongs under English law — defamation and copyright infringement — first charting their historical development and then evaluating their modern expansion and application in cases involving internet intermediaries as defendants. This research identifies an underlying enforcement policy which, complemented by statutory limitations and defences, insulates faultless conduits from monetary liability. It argues that this policy is desirable and

warrants strengthening. Second, this research examines two injunctive remedies — disclosure of the wrongdoer's identity and restricting access to tortious material by means of a new non-facilitation remedy — which complement immunity from substantive liability, but which must be appropriately limited to preserve the rights and freedoms of internet users, innovators and intermediaries.

1 Overview

This research is divided into three parts. Part 1 is introductory. This chapter provides an overview of the research and situates it within recent trends and literature concerning internet regulation and enforcement. It then defends the chosen scope and methodology, and identifies the problems of secondary liability and online enforcement that will be addressed. Chapter 2 introduces the concept of an internet intermediary and makes two arguments. First, it suggests that existing definitions fail to delineate the full spectrum of actors which operate at different layers of the internet's architecture and the different ways they can facilitate and participate in wrongdoing. Second, it proposes a taxonomy based on the OSI network layer model, which better classifies intermediaries according to their functional contributions to harm. Chapter 3 discusses what is meant by 'liability' in the context of claims against internet intermediaries. It sets forth an account of what will here be termed 'secondary liability' as a set of liability-augmenting and limiting doctrines in English and European law. It then explains the normative justifications for imposing civil liability on parties who are not the most proximate causes of wrongdoing.

Part 2 analyses and applies secondary liability rules in two areas of civil wrongdoing. Chapter 4 addresses defamation. It begins with an account of the traditional 'publication' criterion, which delimits legal responsibility for the dissemination of defamatory statements, before considering how this criterion has been applied to secondary internet publishers. It identifies emerging limits in the common law concept of publication which insulate network-layer intermediaries from *prima facie* liability. These are complemented by statutory safe harbours and defences. Chapter 5 applies a similar structure to copyright law and observes that doctrines of 'authorisation' and joint tortfeasorship operate analogously to delimit responsibility for primary infringements carried out by others. Like publication, these concepts have begun to contract, but they have been paired with an emerging class of regulatory obligations under graduated response schemes. As presently conceived, these schemes pose serious concerns for intermediaries' and internet users' rights, but have the potential to operate proportionately.

Part 3 evaluates two complementary responses to intermediaries' participation in internet wrongdoing and proposes several reforms designed to create more effective and proportionate non-monetary remedies. Chapter 6 defends the duty owed by intermediaries to disclose information about third party wrongdoers, arguing that disclosure obligations — when balanced against users' and intermediaries' rights and supported by appropriate procedural safeguards — are logical corollaries of their immunity from primary monetary liability. Chapter 7 sketches the form of a new injunctive remedy to require intermediaries to cease facilitating infringements; in particular, by de-indexing or blocking access to material proved to be tortious but which cannot practicably be removed by other means, and by withholding financial payments from tortfeasors. Although legitimate concerns surround the effectiveness, cost and accuracy of existing blocking technologies, preventing or restricting access to information and assets is sometimes necessary to protect claimants' fundamental rights. Properly limited, such remedies can be proportionate means of enforcing private rights online.

Chapter 8 concludes that there are good doctrinal and policy justifications for limiting or excluding intermediaries' monetary liability for wrongdoing initiated by third parties on the internet. However, to complement those limits, it recommends the availability of the non-monetary enforcement orders proposed in part 3. These orders must be carefully limited by reference to internet users' fundamental rights and freedoms, with costs ordinarily to be paid by the claimant and notice given to all affected parties where appropriate. Taken together, these injunctive remedies offer a powerful toolkit with which to uphold the rule of law on the internet and provide meaningful relief to claimants. However, their limitations must be borne in mind: they will never be completely effective at preventing internet wrongdoing, occluding access to tortious material or compensating claimants; enforcement should be territorially limited; and their application must be shaped by considerations of proportionality, innovation, internet architecture and the rights of intermediaries and their users. Nevertheless, it is suggested that this is one practical path towards achieving a fairer balance between these interests while respecting fundamental properties of the internet's design and preserving open, transparent and neutral conduits for information.

2 The rise of internet intermediaries

The internet is now ubiquitous. Its constituent systems, networks and protocols are essential if not always apparent features in daily life. For a majority of Britons, the internet is now their first

source for locating information,[1] with most consulting search engines and Wikipedia at least eight times each day.[2] Over half use Facebook and other social intermediaries to communicate with friends and conduct human relationships; one third sell goods or services using online marketplaces such as eBay.[3] Public sector cuts have seen growth in government services delivered online.[4] Productivity tools such as online banking, e-mail and telephony produce an average of 144.8 billion daily messages sent to 3.4 billion email addresses.[5] Over a billion people share information via hosted weblogs and media sharing platforms.[6] Internet services are, in short, pervasive and indispensable to our social, economic and political lives.

By design, this infrastructure uses intermediaries to create, store and transmit information, so that internet users depend upon a growing number of parties for access to online content and services. Whenever a person accesses a website, their browser will use (1) a connection supplied by an Internet Service Provider ('ISP') to query (2) a Domain Name System ('DNS') server and determine the domain name's Internet Protocol ('IP') address. Google's DNS server alone processes over 70 billion requests per day.[7] Upon receiving a response, the browser will request the webpage from (3) the remote host on which it is stored, which will then transmit the data back to the user's terminal. In practice, many other intermediaries are interposed: network operators, payment providers, fora, proxies, platforms, cyber-lockers and domain name registrars, among others. These internet resources are recognised as critical national infrastructure,[8] upon which energy, healthcare and transportation services depend.[9] They are increasingly regarded as basic utilities akin to water or electricity.[10] When intermediaries supply these services, they deal with substantial quantities of information authored, edited and uploaded by others.[11]

---

1 William Dutton and Grant Blank, *Next Generation Users: The Internet in Britain* (2011) 22.

2 Alexa Internet Inc, 'Statistics Summary for wikipedia.org' (21 February 2011) <http://www.alexa.com/siteinfo/wikipedia.org>.

3 Office for National Statistics, *Internet Access — Households and Individuals* (31 August 2011) 3–4.

4 National Audit Office, *Government on the Internet: Progress in Delivering Information and Services Online* (13 July 2007) 23, 32.

5 Sara Radicati (ed), *Email Statistics Report, 2012–2016* (April 2012) 3.

6 See, eg, Geoffrey Fowler, 'Facebook: One Billion and Counting' (4 October 2012, *The Wall Street Journal*); Lauren Hockensen, 'Tumblr Numbers: The Rapid Rise of Social Blogging' (14 November 2011, *Mashable Social Media* (reporting 38,000 posts per minute on Tumblr) <http://mashable.com/2011/11/14/tumblr-infographic>.

7 Jeremy Chen, 'Google Public DNS: 70 billion requests a day and counting' (14 February 2012) *The Official Google Blog* <http://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html>.

8 Paul Cornish et al, *Cyber Security and the UK's Critical National Infrastructure* (September 2011) 2.

9 Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (2009) 12.

10 See, eg, European Parliament, MEMO/09/491, annex 1.

11 By one estimate, they transmit, store and cache as much as 67 terabytes of data per second: TeleGeography, *Global Bandwidth Research Service* (2011) 1.

Intermediaries continue to grow in complexity and catalyse national economic growth. By one estimate, Google's index doubled in size to 40 billion pages since 2009,[12] while the total number of indexed Uniform Resource Locators ('URLs') exceeded 1 trillion in 2008 and has since exceeded useful estimation.[13] ISPs connect 77 per cent of British households, while access via mobile handsets has doubled in the past year.[14] Few classes of actors have so rapidly acquired such importance to the national economy. One report estimated the contribution of the communications sector at 4.1 per cent of the United Kingdom's GVA, of which 2.4 per cent consisted of telecommunications intermediaries and 1.7 per cent of internet content intermediaries.[15] Another report estimated their contribution at 5.4 per cent of GDP and concluded that they have accounted for 23 per cent of British economic growth during the previous five years, and 21 per cent in other developed economies.[16]

The economic and social impact of intermediaries has been closely analysed by a growing body of scholars, and this research does not reproduce that work or contribute to the wider policy debates about internet regulation or governance. Instead, the following sections seek to reframe the process of internet rule-making as an iterative contest in which public and private actors seek to determine, among other things, secondary liability rules favourable to their business models and interests. For convenience, we divide the recent history of the internet into four distinct phases: (1) *disintermediation*, in which 'cyberspace' and its actors were treated as an unregulated anarchy of open communication; (2) *protection*, in which territorial content regulation coagulated and intermediaries acquired immunity from certain forms of liability through a patchwork of safe harbours; (3) *expansion*, in which new liability rules developed in national and international institutions; and (4) *balancing*, in which the clamour for stronger enforcement encountered limitations in the fundamental rights of intermediaries and users.

These phases do not have clear chronological boundaries and they can be described in different ways. Palfrey, for example, conceives of an initially open internet becoming progressively more closed and regulated, followed by resistance from technology firms and

---

[12] Maurice de Kunder, 'The Size of the World Wide Web (The Internet)' (18 February 2012) <http://www.worldwidewebsize.com/>.

[13] Jesse Alpert and Nissan Hajaj, 'We Knew the Web Was Big…' (25 July 2008) *The Official Google Blog* <http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html>.

[14] Office for National Statistics, above n 3, 3–5.

[15] Frontier Economics, *Contribution of the Digital Communications Sector to Economic Growth and Productivity in the UK* (2011) 7, 36.

[16] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011) 15–16.

consumer groups.[17] Spar describes how technology lifecycles follow a cyclical pattern containing phases of innovation, commercialisation, creative anarchy and finally rule-making.[18] She suggests that the internet is currently in a state of 'creative anarchy', characterised by conflict between established industries and new uses of digital technology. Benkler, meanwhile, sees the process as a battle for 'control over the basic resources needed to create, encode, transmit, and receive information, knowledge, and culture in the digital environment.'[19] However this process is described, the boundaries of liability faced by intermediaries have been its central though under-acknowledged features.

2.1 Disintermediation: cyberspace as unregulated anarchy

During the early years of the networked society, the internet was an open and largely unregulated medium. In the United States, intermediaries were granted immunity from most forms of tortious liability.[20] These safe harbours were interpreted broadly — mostly in the context of defamation actions against ISPs and bulletin boards.[21] American scholarship tended to fall into two schools. The first questioned the legitimacy of national governments laying claim to sovereignty over internet services at all, since they might not be localisable to particular physical dominions.[22] The second argued that regulation was unnecessary because the internet would inevitably usher in a new age of democratisation and global prosperity.[23] Intermediaries were seen as harbingers of freedom — pioneers and colonists in a new world whose unfamiliar conditions warranted special legal treatment:[24] 'cyberlaws' for 'cyberspace'.[25]

---

17 John Palfrey, 'Four Phases of Internet Regulation' (2010) 77 *Social Research* 981.

18 Debora Spar, *Ruling the Waves: Cycles of Discovery, Chaos and Wealth from the Compass to the Internet* (2001) 11–20.

19 Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (2006) 384.

20 See *Communications Decency Act 1996* (US) 47 USC § 230.

21 See, eg, *Cubby Inc v CompuServe Inc*, 776 F Supp 135 (SDNY, 1991); *Blumenthal v Drudge*, 992 F Supp 44 (DDC, 1998); *Zeran v America Online Inc*, 129 F 3d 327 (4th Cir, 1997). See also *Religious Technology Center v Netcom On-Line Communication Services*, 907 F Supp 1361 (ND Cal, 1995) (copyright).

22 See, eg, John Barlow, 'A Declaration of the Independence of Cyberspace' (8 February 1996) <http://projects.eff.org/~barlow/Declaration-Final.html>; cf Lawrence Lessig, 'The Path of Cyberlaw' (1996) 104 *Yale Law Journal* 1743, 1744.

23 See, eg, I Trotter Hardy, 'The Proper Legal Regime for "Cyberspace"' (1994) 55 *University of Pittsburgh Law Review* 993, 994–5; David Johnson and David Post, 'Law and Borders — The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367.

24 See, eg, William Blackstone, *Commentaries on the Laws of England* (9th ed, 1783, reprinted 1978) vol 1, 108; Alex Castles, 'The Reception and Status of English Law in Australia' (1963) 2 *Adelaide Law Review* 1, 5–6.

25 See, eg, Frank Easterbrook, 'Cyberspace and the Law of the Horse' [1996] *University of Chicago Legal Forum* 207. Cf Julie Cohen, 'Cyberspace as/and Space' (2007) 107 *Columbia Law Review* 210, 212–13.

The global ecology of intermediary liability was therefore one of optimistic denial: intermediaries would not be regulated directly; instead, their code would be regulated — largely by market forces — and that code would in turn define the new borderless world.[26] Certainly, very little evidence exists of early internet litigation or legislation in the United Kingdom.[27] Even as metaphors borrowed from physical space found acceptance,[28] a tendency emerged to treat the internet as intrinsically different from other information revolutions. Unlike print, radio and television, the internet enabled many-to-many communication and not simply one-to-many broadcasting. Networked communications thus reversed a trend, observable for at least 150 years, towards the simultaneous expansion of information dissemination and the concentration of its production among a handful of increasingly powerful industries.[29]

Despite being right about the enormity of these changes to production and dissemination, the cyber-anarchists were wrong in three crucial respects. First, the internet did not bring about the widespread disintermediation assumed by many 'cyber-anarchists'.[30] By the close of the 20th century, intermediation had increased sharply as consumers turned to search engines, ISPs, online marketplaces and portals to reduce the transaction costs associated with navigating the exaflood of data, identifying relevant information, and measuring its reliability. Second, the internet did not come to be accepted as a 'Wild West' in which wrongdoing was incapable of regulation.[31] Online activities were mediated by a limited group of powerful facilitators, who proved 'no less amenable' to being gatekeepers for various civil wrongs.[32] Third, most wrongdoing carried out online was not new and remained harmful. As Solove reminds us: 'Gossip, rumor, and shaming have been with us since the dawn of civilization.'[33] Technology has also long facilitated unauthorised copying; in the mid-18th century, authors complained of the diffusion of 'surreptitious and pyrated' editions,[34] while Defoe predicted 'a general Rapsody of Piracy, Plagiarism, and Confusion.'[35] In Victorian England, increases in print dissemination brought about by advances in plate technology, telegraphy and economies of scale brought us tabloids,

---

26 See, eg, Lawrence Lessig, *Code and Other Laws of Cyberspace* (2nd ed, 2006) 122–5.

27 See *Shetland Times v Willis* [1997] SC 316 (copyright); *Godfrey v Demon Internet Ltd* [2001] QB 201 (defamation).

28 See, eg, Jane Ginsburg, 'Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace' (1995) 95 *Columbia Law Review* 1466.

29 Benkler, above n 19, 29–32.

30 Cf OECD, *The Economic and Social Impact of Electronic Commerce* (1999) 24.

31 See Assaf Hamdani, 'Who's Liable for Cyberwrongs?' (2001) 87 *Cornell Law Review* 901, 902; Michael Meyer, 'Crimes of the "Net"' (13 November 1994, *Newsweek*, New York).

32 Tim Wu, 'When Code Isn't Law' (2003) 89 *Virginia Law Review* 679, 717.

33 Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (2007) 105.

34 See Adrian Johns, *Piracy: The Intellectual Property Wars from Gutenberg to Gates* (2009) 46–7.

35 Daniel Defoe, 'Miscellanea' (3 December 1709) 104 *Review VI* 415.

penny-presses and their 'high-spiced wares'.[36] In trade marks, '*piraterie pharmaceutique*' is documented as early as 1812.[37] The arrival of the internet did not fundamentally change these old wrongs, but merely multiplied their potential consequences and made it harder to identify and enforce rights against their perpetrators.

2.2 Protection: territorial fragmentation and horizontal safe harbours

The fourth reality to emerge from the nascent information economy was that acts which occur on the internet were readily localisable to physical space. Intermediaries were not actors in ethereal cyberspace, but local entities which acted through physical machines to cause tangible harms in specific places.[38] Internet content became territorially fragmented as geolocation and filtering technology allowed intermediaries to avoid liability under disharmonised censorship regimes in both developing and developed countries.[39] For example, access could be restricted in regions where publication of material may be a contempt of court[40] or infringement of copyright.[41] The emergence of territorial localisation ensured that technological limitations would not displace the rule of law entirely. However, most scholars accepted that intermediaries must be shielded from at least some of the liability which they might otherwise face under conventional, 'offline' liability rules.

The literature of this period offers four common justifications. First, to hold intermediaries liable for all harms facilitated by their services would impose an impossible monitoring burden, given the rate at which new information is uploaded and transmitted.[42] For example, YouTube receives more than 72 hours of video per minute,[43] while Facebook transmits over 15 billion user-uploaded photographs per day.[44] Even the most advanced algorithms cannot determine whether

---

[36] Charles Dickens, *The Life and Adventures of Martin Chuzzlewit* (1844 ed) 200.

[37] See A P Favre, *De la Sophistication des Substances Médicamenteuses, et des Moyens de la Reconnaître* (1812) x–xi.

[38] See, eg, *Dow Jones & Co Inc v Gutnick* (2002) 210 CLR 575; Orin Kerr, 'The Problem of Perspective in Internet Law' (2003) 91 *Georgetown Law Journal* 357, 360–3.

[39] See Catherine Stromdale, 'Regulating Online Content: A Global View' (2007) 13 *Computer and Telecommunications Law Review* 173, 174.

[40] Eg, Tom Zeller, 'Times Withholds Web Article in Britain' (*The New York Times*, 29 August 2006) <http://www.nytimes.com/2006/08/29/business/media/29times.html>.

[41] Eg, British Broadcasting Corporation, 'Can I Use BBC iPlayer outside the UK?' (22 February 2012) *BBC* <http://iplayerhelp.external.bbc.co.uk/help/outside_the_uk/outsideuk>.

[42] See, eg, Lilian Edwards and Charlotte Waelde, 'Online Intermediaries and Liability for Copyright Infringement' (Paper presented at the World Intellectual Property Organization, Geneva, 2005) 15–16.

[43] YouTube LLC, 'YouTube Trends' (23 January 2012) *The Official YouTube Blog* <http://youtube-global.blogspot.com/2012/01/holy-nyans-60-hours-per-minute-and-4.html>.

[44] Doug Beaver, '10 Billion Photos' (15 October 2008) *Facebook* <http://facebook.com/note.php?note_id=30695603919>.

a statement is defamatory, a photograph is used for fair dealing, or information is confidential. To require intermediaries to bear liability in these circumstances would, it was argued, be unfair and require an unfeasibly large investment to review and quarantine tortious content. The second reason for limiting liability was to discourage excessive monitoring of networks and overzealous removal of potentially tortious content, which might chill speech and endanger privacy.[45] Third, conscripting intermediaries to police content was seen as inconsistent with their technical status as neutral conduits. Deep philosophical resistance emerged to the idea of forcing gatekeepers to regulate internet content,[46] which can partly be understood as a reaction to the enforcement reflex of content industries and governments who sought to control technologies of dissemination. Finally, limiting liability was thought to encourage innovation and economic development, since unlimited liability might deter firms from investing in network infrastructure and online services which created positive externalities.[47]

Liability rules in the United Kingdom were profoundly affected by the transposition of the E-Commerce Directive, which continued a trend towards the Europeanisation of telecommunications and intellectual property policy.[48] Horizontal safe harbours protected intermediaries who act 'passively and neutrally' from nearly all forms of primary liability, but only for specific types of conduct.[49] Under this weak view of immunity, intermediaries enjoyed immunity only until they received knowledge of wrongdoing or intervened in transmission, at which point they came under an obligation to remove or restrict access to the material. This created a paradox whereby intermediaries had strong incentives not to intervene. As will be seen in chapter 3, the Directive failed to harmonise secondary liability and national courts have construed the safe harbours inconsistently and often narrowly.

---

45 Hamdani, above n 31, 909–21; cf Doug Lichtman and Eric Posner, 'Holding Internet Service Providers Accountable' (2006) 14 *Supreme Court Economic Review* 221, 225–6.

46 Jane Strachan, 'The Internet of Tomorrow: The New–Old Communications Tool of Control' (2004) 26 *European Intellectual Property Review* 123, 124.

47 See Lauren Patten, 'From Safe Harbor to Choppy Waters: YouTube, the *Digital Millennium Copyright Act*, and a Much Needed Change of Course' (2007) 10 *Vanderbilt Journal of Entertainment and Technology Law* 181, 208–10.

48 Davor Jančić, 'The European Political Order and Internet Piracy: Accidental or Paradigmatic Constitution-Shaping?' (2010) 6 *European Constitutional Law Review* 430, 438.

49 See below chapter 3, § 2.1. See also Jeremy de Beer and Christopher Clemmer, 'Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries' (2009) 49 *Jurimetrics* 375, 377.

2.3 Expansion: new types of secondary liability

Intermediaries had hitherto existed in largely independent, function-specific spheres, functioning as feudal kingdoms with their own systems of membership, regulation and privileges.[50] Outside their walls, technology companies entered a battle with content industries to enclose and 'propertise' the electronic commons: the winner would get to define favourable liability rules to regulate information and its conduits; the loser would need to internalise the cost of user misbehaviour. However, as the networked information economy evolved, content, reputation, property and identity became increasingly disaggregated in ways that threatened to upset incumbent industries[51] and traditional methods of enforcing legal rights. In parallel, the largest internet platforms were aggregating services and growing rapidly in size and power.

As the quantity of online material grew, so did the prevalence of tortious content and services enabling its creation and dissemination. A growing corpus of scholars argued that because internet industries were coming of age, early policies of immunity were no longer necessary to encourage growth.[52] Because there was often no better defendant, they argued, it was reasonable to use liability rules to create *ex ante* incentives for intermediaries to police misconduct where they had the technological capacity to do so and the cost of preventative steps was less than the overall reduction in harm. Claimants found it increasingly difficult to remove tortious content, which grew like hydra: every website or service removed spawned two new imitators.[53] Scholars heaped criticism upon broad American immunities from tort liability,[54] observing that free expression was increasingly mediated and filtered by a select group of commercially-motivated intermediaries.[55] Others criticised the 'Streisand effect', whereby attempts to remove material merely drew unwanted attention to it,[56] and the difficulty of obtaining meaningful redress against anonymous tortfeasors.

---

[50] Alfred Yen, 'Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace' (2002) 17 *Berkeley Technology Law Journal* 1207, 1239–43.

[51] See Benkler, above n 19, 32.

[52] See, eg, Ronald Mann and Seth Belzley, 'The Promise of Internet Intermediary Liability' (2005) 47 *William and Mary Law Review* 239, 274–5; Lichtman and Posner, above n 45.

[53] See Herbert Rose, *A Handbook of Greek Mythology* (1990) 174. See also Karl Kerényi, *The Heroes of the Greeks* (1978) 143–4 (describing the hydra's regenerative properties in Greek mythology).

[54] See *Communications Decency Act 1996* (US) 47 USC § 230 (tort); *Digital Millennium Copyright Act 1998* (US) 17 USC § 512 (copyright) ('*DMCA*'); *Lanham Act* (US) s 32(2); 15 USC § 1114(2) (trade marks).

[55] See, eg, Anne Cheung and Rolf Weber, 'Internet Governance and the Responsibility of Internet Service Providers' (2008) 26 *Wisconsin International Law Journal* 403, 411.

[56] See Andy Greenberg, 'The Streisand Effect' (11 May 2007) *Forbes* <http://www.forbes.com/2007/05/10/streisand-digg-web-tech-cx_ag_0511streisand.html>.

When copyright enforcement against primary infringers began to fail,[57] claimants sought to target points of dissemination from which infringing material was located, distributed and exchanged. This was a 'seismic shift' in enforcement strategy,[58] which saw the emergence of new theories of secondary liability principally to deal with operators of peer-to-peer ('P2P') file-sharing networks. During this period, several generations of P2P protocols were created, sued and forced into bankruptcy or closure.[59] Each sought to evade the operation of gatekeeper enforcement regimes by employing increasingly decentralised network designs, but in doing so they inevitably introduced new intermediaries. No peer distribution system, it emerged, was entirely 'pure'; someone was always needed to supply network access and infrastructure, maintain an index of files and peer nodes, and distribute client software.

In conjunction with self-regulation, the expanded secondary liability rules applied in actions between private litigants became *de facto* regulators of new internet technologies, communications,[60] business models, consumer rights and speech.[61] Policymakers tended to respond to this expansion in three ways. The first group sought to reconceptualise primary wrongdoing in a way that better reflected the needs of technology, users and intermediaries, particularly in the context of internet copyright enforcement. Thus, in the United Kingdom, the *Gowers Review* and *Hargreaves Review* recommended the modernisation of primary liability rules for the internet, while recommending that ISPs assist their enforcement.[62] The second group opposed regulatory 'exceptionalism' and justified the retention of existing legal norms by reference to theories of law and economics.[63] Intermediaries were seen as gatekeepers to whom liability incentives could properly be applied if they were the least cost avoiders of harm. The third group sought to develop new methods for detecting and deterring copyright infringement, leading to the enactment of *sui generis* 'graduated response' and notification schemes.[64]

---

[57] See chapter 5, § 2.6 for discussion of the reasons.

[58] Mark Lemley and R Anthony Reese, 'Reducing Digital Copyright Infringement Without Restricting Innovation' (2004) 56 *Stanford Law Review* 1345, 1353.

[59] See, eg, *A & M Records v Napster Inc*, 239 F 3d 1004, 1022 (9th Cir, 2001) (Napster); *In re Aimster Copyright Litigation*, 334 F 3d 643 (7th Cir, 2003) (Aimster); *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd*, 545 US 913 (2005) (Grokster); *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 65 IPR 289 (KaZaA).

[60] See Timothy Wu, 'Copyright's Communications Policy' (2004) 103 *Michigan Law Review* 278.

[61] See Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth* (2011) 47.

[62] Andrew Gowers, *Gowers Review of Intellectual Property* (2006) 103.

[63] See Hamdani, above n 31; Douglas Lichtman and William Landes, 'Indirect Liability for Copyright Infringement: An Economic Perspective' (2003) 16 *Harvard Journal of Law and Technology* 395; Mann and Belzley, above n 52; Lichtman and Posner, above n 45.

[64] See Ira Nathenson, 'Civil Procedures for a World of Shared and User-Generated Content' (2010) 48 *University of Louisville Law Review* 911; Greg Lastowka, 'Google's Law' (2007) 73 *Brooklyn Law Review* 1327.

The overall ecosystem of online wrongdoing evolved in what some described as an 'arms race' between claimants, innovators and tortfeasors.[65] *Ex post* liability rules expanded to accommodate new distribution technologies which threatened existing economic practices and social expectations. Faced with this interminable cycle of regulation and circumvention, some courts lamented the 'quicksilver technological environment with courts ill-suited to fix the flow of internet innovation'.[66] In parallel, secondary liability rules were placed on the international trade agenda and propagated throughout the world by means of free trade agreements, bilateral investment treaties and new multilateral agreements designed to export American 'gold standards' of liability.[67]

2.4 Balancing: enforcement and vertical integration

Most recently, secondary liability rules have developed new limits derived from fundamental rights and principles of free trade.[68] As the European Parliament has reminded member states, enforcement measures against intermediaries must not 'conflict[…] with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness'.[69] This phase is characterised by a departure from *ex post* liability under monetary liability rules in favour of *ex ante* prevention using non-monetary obligations enforced by injunction. European balancing criteria place upper limits on the terms of such relief, though many scholars have criticised them as creating a 'messy legal fog'.[70] Civil society groups have been particularly active in resisting stronger enforcement, mobilising to develop charters of internet rights and oppose legislation and trade agreements perceived as contrary to internet freedom.[71] These developments reflect a gradual recalibration towards more balanced intermediary liability rules.

These trends have led internet regulation away from judicial incrementalism towards co-regulatory and legislative models, whose implications are not yet fully understood. Scholars

---

65 See Lee Kovarsky, 'A Technological Theory of the Arms Race' (2006) 81 *Indiana Law Journal* 918, 932–6.

66 *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd*, 380 F 3d 1154, 1167 (9th Cir, 2004); overruled, 545 US 913 (2005).

67 See, eg, Trans-Pacific Partnership Agreement (Draft text of February 2011); Annemarie Bridy, 'ACTA and the Specter of Graduated Response' (2011) 26 *American University International Law Review* 559. See Robert Burrell and Kimberlee Weatherall, 'Exporting Controversy? Reactions to the Copyright Provisions of the US-Australia Free Trade Agreement: Lessons for US Trade Policy' [2008] *Journal of Law, Technology and Policy* 259, 294–8.

68 See generally chapter 3, § 2.

69 European Parliament, *Resolution on Cultural Industries in Europe* (2007/2153(INI)).

70 Franceso Rizzuto, 'European Union Telecommunications Law Reform and Combating Online Non-Commercial Infringements of Copyright: Seeing through the Legal Fog' (2011) 17 *Computer and Telecommunications Law Review* 75, 92.

71 See, eg, Internet Rights and Principles Coalition, *Charter of Human Rights and Principles for the Internet* (2011); Stop Online Piracy Bill 2012 (US) (HR 3261).

continue to argue that wider liability would 'disrupt the existing Internet ecosystem to a degree that could stifle overall progress'.[72] However, there is little empirical analysis or consensus about the wider effects of liability upon content, innovation and freedoms. Instead, the limits of responsibility are being specified by reference to doctrines imported from public and European law. This reflects the reality that the 'internet' is no longer a distinct regulatory subject, but broadly coterminous with other areas of law. Intermediaries have lost their status as vulnerable innovators in need of protection from incumbents and are instead being viewed as both victims and *agents* of wrongdoing.

This adjustment follows two important changes: first, with the emergence of 'web 2.0' platforms and cloud computing,[73] users are increasingly vulnerable to decisions by intermediaries that affect their welfare, just as technical and architectural design choices can dictate the utility of those platforms. Second, intermediaries' incentives are changing, as vertical integration and network effects transform them into the incumbents they once unseated.[74] Intermediaries often operate in two-sided markets characterised by strong network effects, which has led some scholars to challenge the dominant positions enjoyed by firms such as Google[75] and Facebook.[76] Those intermediaries now possess unparalleled power to influence the reputation,[77] free expression,[78] personal information[79] and property rights[80] of others.

In short, the battle to define the scope of secondary liability rules and, indirectly, the functions and limits of internet technology, continues to be waged. Because of their central position, intermediaries remain the focus of current regulatory efforts and face pressure from claimants and governments around the world to enforce private rights online. Intermediaries seek to reduce the expected costs of compliance through a combination of lobbying and voluntary action.[81] Set against these pressures, an emerging suite of limiting principles, bolstered by community activism, appears to be influencing the normative characteristics of internet

---

72 Marc Aaron Melzer, 'Copyright Enforcement in the Cloud' (2011) 21 *Fordham Intellectual Property, Media and Entertainment Law Journal* 403, 447.

73 See, eg, Edward Lee, 'Warming up to User-Generated Content' [2008] *University of Illinois Law Review* 1459, 1546–7.

74 de Beer and Clemmer, above n 49, 406.

75 See Lastowka, above n 64, 1399.

76 See James Grimmelmann, 'Saving Facebook' (2009) 94 *Iowa Law Review* 1137, 1163.

77 See Solove, above n 33, 155–60.

78 See Seth Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155 *University of Pennsylvania Law Review* 11, 16.

79 See Jonathan Zittrain, 'Privacy 2.0' [2008] *The University of Chicago Legal Forum* 65, 110, 115.

80 See Wu, above n 60, 340–1, 344.

81 See Wu, above n 32, 688–95.

communications — 'who gets to say what, to whom, and who decides?'[82] — and forging an unsteady, contested equilibrium between the social and economic practices of intermediaries, and the rights of claimants and users.

3 Remedies against internet intermediaries

The previous section identified a worldwide shift in the attribution of liability for internet misconduct from primary to intermediary wrongdoers and from monetary to non-monetary remedies. The enforcement policies reflected in these trends are complex and dynamic, and will be examined more closely in later chapters. Partly, they can be explained as examples of the regulatory impulse to impose liability upon messengers[83] and other bearers of bad news.[84] They also reflect invisible legislative, adversarial, technical and market forces, which in turn share close relationships to the evolution of technologies for creating and disseminating information. The purpose of this section is to introduce the different enforcement methods considered by this research and to understand why they are sought against intermediaries rather than (or in addition to) primary wrongdoers.

3.1 Reasons for targeting intermediaries

A preliminary objection is: why should the law concern itself with intermediaries? Wrongdoing, it might be argued, is committed by specific individuals; focus is therefore better fixed upon the acts of those users and the primary liabilities to which they give rise. A fuller defence of why intermediaries and other secondary parties are proper subjects of regulation will be given in chapter 3. At this stage, it suffices to identify four practical reasons why claimants target intermediaries notwithstanding that there may exist another responsible party: first, the inability of *primary tortfeasors* to compensate harm; second, the *visibility and local presence* of many intermediaries, who present attractive regulatory bottlenecks when compared to anonymous or judgment-proof primary tortfeasors; third, the *collateral effects* of remedies upon the policies and services of platforms; and fourth, lower *enforcement costs*. These reasons are examined in turn.

---

[82] Benkler, above n 19, 392.

[83] See William Shakespeare, *The Tragedy of Coriolanus* (1608) IV:vi, Menenius ('You shall chance to whip your Information, // And beate the Messenger, who bids beware Of what is to be dreaded').

[84] See Sophocles, *Antigone* (2003 ed, Reginald Gibbons and Charles Segal trans) II:310 ('no one loves // A messenger who brings with him bad news').

(a) *Inadequacy of primary wrongdoers*

The internet makes it disproportionately easy for people to cause harm on orders of magnitude greater than their ability to compensate the resulting losses. Almost any information can be instantaneously transmitted to a public forum, which can be cheaply located by anyone using search engines and other gateways. Defamatory rumours, confidences and infringing material propagate virally on gossip blogs and discussion boards, assisted by two social phenomena: *social cascades*, by which informational signals given by others propagate beliefs; and *polarisation*, by which group deliberation amplifies individual responses.[85] For example, repeated exposure to a salacious rumour increases its likelihood of being further disseminated, and copyright infringers are more likely to believe their actions are justified if they observe others behaving in the same way. These three properties — the low cost of dissemination, the tendency for viral cascades and amplification, and the scale with which tortious information can be reproduced — mean that damage can be caused on a large scale with relatively little effort.

The originator of a false rumour or infringing file which is subsequently read or copied by millions of people will rarely possess assets sufficient to compensate claimants for their losses. Besides the damage caused by publication itself, the permanence of many internet materials has lingering consequences: victims of internet defamation may have statements used against them in future job applications; copyright owners may be unable to control or commercially exploit a work. In these circumstances, deep-pocketed intermediaries present attractive targets for claimants who seek to recover losses above and beyond what the primary tortfeasor is able to pay. Claimants accordingly turn to intermediaries to insure against the risk of catastrophic, amplified harms arising from online activities.

(b) *Visibility and presence*

Second, intermediaries tend to be more easily identifiable than primary tortfeasors. Many operate fixed infrastructure in multiple jurisdictions and play highly visible roles in internet communications; with some notable exceptions, they make no effort to hide their ownership or identity. Indeed, those that wish to avail themselves of safe harbours must publish information about their own identity and location, which ensures they are able to be identified.[86] Conversely,

---

[85] See Cass Sunstein, 'Believing False Rumors' in Saul Levmore and Martha Nussbaum (eds), *The Offensive Internet: Speech, Privacy, and Reputation* (2010) 91, 92, 96.

[86] *E-Commerce Regulations* reg 6(1), (2).

it may be costly or even impossible to discover the true identity of the primary tortfeasor.[87] While their concealment is often imperfect,[88] anonymity tends to be most endemic in the realm of intentional content torts, many of which occur on platforms which permit pseudonymous registration. As Rustad and Koenig argue, if such intermediaries face no liability at all, entire categories of online wrongdoing may go uncompensated, since no other solvent wrongdoer can be identified.[89] Intermediaries are also more likely to have a physical presence in the claimant's jurisdiction, which may make it cheaper to bring proceedings and enforce judgment against local assets.[90] For example, an ISP will almost always have a domestic presence in any region where it supplies access to customers. The individual tortfeasor may be beyond jurisdiction, domiciled in a third country or have no assets present in the forum.

(c) *Collateral effects*

An intermediary may be able to put an end to tortious activity in a way that targeting individual tortfeasors cannot. This potential arises from the capacity of many intermediaries to detect, prevent and control the means of wrongdoing at the disposal of tortfeasors; for example, by monitoring future instances of infringement, suspending or terminating user accounts, or altering platform functionality. Remedies against intermediaries mobilise their regulatory potential against future tortfeasors in order to police the successful claimant's rights. Powerful injunctive remedies may require intermediaries to alter their technology or even business models and thereby to internalise the costs of wrongdoing. This makes them attractive tools for claimants to influence many users' behaviour simultaneously. Claimants understandably prefer these pre-emptive mechanisms to *ad hoc* loss shifting against individual defendants, since orders against one primary wrongdoer will not necessarily prevent or deter others from undertaking similar activity. It is this potential to compel *ex ante* regulation of future losses that makes intermediaries such attractive sources of relief. However, actions against intermediaries are in one sense more limited, since their formal effects are usually limited to the defendant's own services, whereas relief against primary tortfeasors may be broader.

---

87 See Verizon Communications Inc, *2012 Data breach Investigations Report* (2012) 20.

88 See, eg, Jonathan Mayer, '"Any Person … a Pamphleteer": Internet Anonymity in the Age of Web 2.0' (7 April 2009) 30–1; Arvind Narayanan et al, 'On the Feasibility of Internet-Scale Author Identification' [2012] *IEEE Symposium on Security and Privacy* 300.

89 Michael Rustad and Thomas Koenig, 'Rebooting Cybertort Law' (2005) 80 *Washington Law Review* 335, 346, 350.

90 See Chris Reed, 'Think Global, Act Local: Extraterritoriality in Cyberspace' (Research Paper No 58/2010, Queen Mary University of London) 2.

(d) *Cost*

Suing individual tortfeasors is generally feasible only where a small number of people have committed wrongdoing. Where tortious information is being propagated by tens of thousands of people on a platform, it is likely to be far more cost-effective for a claimant to target the operator of the platform. In general, if claimants can obtain an effective remedy from such a gatekeeper, that will entail lower enforcement costs than taking steps to identify and enforce judgments against every tortfeasor. The potential for secondary liability rules to reduce claimants' enforcement costs (as well as *ex post* negotiation costs with intermediaries)[91] is discussed further in chapter 3.

3.2 Monetary remedies

This research is only concerned with civil liability, which gives rise to two main classes of remedies. First, remedies for liability can be monetary, as in the case of orders to pay damages or disgorge profits.[92] Such orders enforce secondary duties to correct losses or gains arising from breach of a primary duty. These obligations to pay are backed by the threat of executive enforcement and asset seizure. This research does not comment on the justification for these remedies or the principles governing their quantification. It suffices to note that almost all information torts recognise an obligation on the legally responsible party to pay money.[93] Preconditions for monetary remedies can be broadly grouped under four headings.

(a) *Strict liability*

First, strict liability requires intermediaries to internalise the cost of user misconduct without proof of fault. By requiring intermediaries to pay for the social harms of third party wrongdoing, tort law increases the expected penalty — and thereby the deterrent effect — of facilitating that wrongdoing, with the effect that intermediaries adjust their activities to reduce wrongdoing to an optimal level.[94] Strict liability has the advantages of being simple for courts and intermediaries to assess, and allowing efficient *ex ante* pricing decisions. However, although strict primary liability

---

91 Hamdani, above n 31, 924.

92 See generally *Attorney General v Blake* [2001] 1 AC 268, 278–81 (Lord Nicholls).

93 See *John v MGN Ltd* [1997] QB 586, 608–9 (Sir Thomas Bingham MR) (defamation); *Copyright Act* ss 96(1), 97–100, 103, 184(2), 191I (copyright infringement).

94 See Jennifer Arlen and Reinier Kraakman, 'Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes' (1997) 72 *New York University Law Review* 687; Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76 *Journal of Political Economy* 169, 178–80, 184.

rules are common, strict secondary liability rules are rare, principally because it is unfeasibly costly for intermediaries to monitor the lawfulness of all users' activities.

(b) *Negligence-based standards*

Second, intermediaries may be required to act reasonably to prevent or deter primary wrongdoing. This represents a lower level of monitoring and reduces the risk of over-deterrence by holding intermediaries to an objectively determined but imperfect standard of conduct — for example, a rule which requires a website operator to remove defamatory postings 'within a reasonable period'.[95] Duties fixed by reference to external standards such as industry practices can operate more stringently than knowledge-based duties; for example, by imputing constructive knowledge of tortious material.

(c) *Knowledge-based standards*

Knowledge-based standards furnish the dominant mechanism for European internet content regulation: notice-and-takedown. They impose obligations upon intermediaries to respond to wrongdoing only once they receive sufficient information to infer that wrongdoing has occurred. Less wrongdoing must be internalised, which encourages optimal *ex post* enforcement. To prevent wilful blindness, knowledge usually incorporates an objective measure.[96] In equitable doctrines, dishonesty-based standards reflect similar but distinct principles, delimiting liability according to whether the defendant's mental state was objectively culpable.[97]

(d) *Immunity*

At the other end of the liability rule spectrum, intermediaries can be fully exempted from monetary liability. Immunity has the advantages of certainty, subsidising nascent technology industries and promoting 'market-based self-help',[98] but has been heavily criticised by American scholars as removing any incentives for least-cost avoiders to intervene in enforcement, even where that might be most efficient[99] or necessary to uphold claimants' rights.

---

95 See, eg, *DesignTechnica*; *Emmens v Pottle* (1885) QBD 354. See below chapter 4, §§ 2.2(b), 3.2(c).

96 See, eg, E-Commerce Directive arts 13(1)(e), 14(1)(b).

97 See below chapter 3, §1.4.

98 Lichtman and Posner, above n 45, 226.

99 Rustad and Koenig, above n 89, 390–1. See also Ronald Mann and Jane Winn, *Electronic Commerce* (2nd ed, 2005) 189.

3.3 Injunctive remedies

Alternatively, intermediaries may be ordered to interdict or prevent third parties' tortious activities. These injunctive remedies are impervious to safe harbours, which 'do not affect the possibility of injunctions of different kinds'.[100] They are enforced, ultimately, by the criminal law of contempt and the associated machinery of incarceration. Liability in this second, non-monetary sense is both broader and narrower: it can be awarded without proof of wrongdoing, but only protects limited categories of interests. Three justifications are commonly given. First, where 'intermediaries are best placed to bring such infringing activities to an end'[101] — in other words, where they are least-cost avoiders — injunctive relief should enforce optimal gatekeeping functions in the event of market failure. Second, there may be circumstances in which the claimant's *Convention* or *Charter* rights are engaged and an injunction is a necessary and proportionate remedy to protect them — subject to various upper limits discussed in chapters 3, 6 and 7. Third, although a facilitator of wrongdoing may not itself be a wrongdoer in law, it may come under an equitable duty to assist claimants to halt that wrongdoing and obtain relief. The following sub-sections outline the seven injunctive remedies relevant to this research.

(a) *Removal*

The most common non-monetary remedy is removal, which simply requires the deletion of tortious content at its source. By 'taking down' such content, the intermediary prevents further dissemination from that location.[102] In practice, removal is imperfect. Copies of material may be cached or mirrored; the claimant may be unable to identify all such copies or enforce orders against every source of the material. Even assuming that all additional copies have been removed, it could easily be re-uploaded by a determined tortfeasor. Moreover, attempts to remove material can often backfire, as the 'Streisand effect' illustrates.[103] Removal is most commonly sought against hosts or content distribution networks. Although normally by court order, it can be voluntary. For example, in December 2010, Amazon removed Wikileaks' cloud storage service following

---

[100] E-Commerce Directive, recital (45).

[101] Information Society Directive, recital (59), art 8. See also Enforcement Directive, recital (23), arts 9(1)(a), 11.

[102] See, eg, E-Commerce Directive recital (45).

[103] See above n 56 and accompanying text.

pressure by the United States government.[104] Removal remedies for defamatory and copyright matter are discussed further in chapters 4 and 5.

(b) *Notification*

Notification involves marshalling intermediaries to send notices to internet users from whom apparently tortious activity is detected. Notices perform two signalling functions: first, they indicate that the activity is wrongful (at least allegedly so), which the wrongdoer may not have realised; and second, like a letter before action, they tell him that somebody is watching his activities and might take further action if they do not cease. This might deter future wrongdoing by elevating the expected penalty. Notification schemes have been enacted or proposed in the United Kingdom, France, Australia, New Zealand, South Korea and United States which require ISPs to forward notices to subscribers alleged to be copyright infringers,[105] with the threat of escalating sanctions. Chapter 5 evaluates their efficacy and proportionality.

(c) *Disclosure*

An intermediary can be ordered to disclose information it holds about potential tortfeasors to enable claimants to pursue some legitimate action against them. The remedy of disclosure was first recognised by courts of equity as a duty enforceable by injunction. Today its boundaries are regulated by data retention, interception and access laws, and by the principle of proportionality. Chapter 6 argues that disclosure is preferable to monetary actions against intermediaries in almost all circumstances, but proposes several reforms designed to strike an appropriate balance between the rights of claimants, intermediaries and internet users.

(d) *Blocking*

Blocking orders require an intermediary to prevent its users from accessing tortious information. This remedy suffers the existence of the tortious information but seeks to curtail its dissemination by preventing individual computers from retrieving it. This is potentially useful where the gist

---

[104] John Naughton, 'WikiLeaks Row: Why Amazon's Desertion has Ominous Implications for Democracy' (*The Guardian*, 11 December 2010) <http://guardian.co.uk/technology/2010/dec/11/wikileaks-amazon-denial-democracy-lieberman>.

[105] See *Digital Economy Act 2010* (UK); Loi n° 2009-669 of 12 June 2009, *Loi Favorisant la Diffusion et la Protection de la Création sur Internet* (FR); Communications Alliance Ltd, *A Scheme to Address Online Copyright Infringement* (2011) 5–8; *Copyright (Infringing File Sharing) Amendment Act 2011* (NZ); Law No 432, *Copyright Act 1957* (KR) art 133-2(2); Center for Copyright Information, 'What is a Copyright Alert?' (26 February 2013) <http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/>.

of the tort lies in the consumption or reproduction of material rather than its existence *per se*. The object of the remedy is not the source host but rather an ISP which supplies internet access to its subscribers. Until recently, this remedy was largely unknown. Blocking technology was expensive, ineffective and largely confined to corporate networks, university campuses and authoritarian states. However, blocking is now emerging throughout Europe and elsewhere as a complementary remedy to notice-and-takedown: if tortious material cannot be removed at its source, it might yet be targeted and curtailed at its destinations. Nevertheless, blocking is attended by a multitude of serious concerns. Most implementations create a risk of *overblocking* — that is, false positives — consisting of the denial of access to material which is not tortious or illegal. Doubts have been expressed about its efficacy,[106] given the potential for *underblocking* and circumvention. Blocking may create wider hazards for freedom of expression, chilling speech and exacerbating problems said to inhabit the scope of primary liability for defamation, privacy and copyright online.[107] It may distort competition between ISPs which afford different levels of access to information. It may even 'break the internet' by interfering in the Domain Name System and intruding upon the layered architecture of communications networks.[108] These and other charges are considered in chapter 7.

(e) *De-indexing*

A de-indexing order obliges an intermediary to remove a hyperlink to tortious material. This remedy is directed at the operators of search engines and aggregators, who must add the affected URLs or websites to a blacklist or 'sandbox' of materials which are no longer to appear in search results. Such orders are almost unknown in England. However, the government has indicated that it intends 'to work with search engines' to deindex 'unlawful sites'.[109] A related remedy is *partial* deindexing or deprioritisation of search results. This would involve actively interfering in a search engine's relevance algorithm to reposition tortious material, without removing that material from the index entirely. Critics have argued that such algorithmic interference violates

---

[106] See OFCOM, *'Site Blocking' to Reduce Online Copyright Infringement* (May 2011) 46–9.

[107] Frank La Rue, United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (May 2011) 9–12.

[108] Mark Lemley, David Levine and David Post, 'Don't Break the Internet' (2011) 64 *Stanford Law Review Online* 34, 35–6.

[109] Department of Culture, Media and Sport, *Next Steps for Implementation of the* Digital Economy Act (2011) 7.

search neutrality and risks distorting competition for search services.[110] A framework for effective and balanced de-indexing remedies is proposed in chapter 7.

(f) *Asset seizure and freezing*

These injunctions require an intermediary to disrupt a tortfeasor's control over electronic and financial resources. First, domain name controllers may be ordered to withhold access to a registrant's domain name. Traffic to that domain name can then be redirected to a new host, such as a warning page[111] or law enforcement 'honeypot'.[112] Domain seizure differs from takedown and blocking orders in that it does not remove the original material but instead appropriates the domain name, which is no longer associated with the material. Unlike blocking orders, users are not prevented from reaccessing that server or the redirected domain name. Seizure is now employed routinely in the United States, where Immigrations and Customs Enforcement and the Department of Justice have seized nearly 84 500 domain names.[113] However, serious criticisms have been made of false positives[114] and limited procedural safeguards governing seizure.[115]

Second, payment intermediaries may be ordered to freeze tortfeasors' assets; for example, to prevent funds from being dissipated, in effect cutting off their monetary supply. The objective is to preserve assets which could be used to satisfy judgment against primary wrongdoers, and also to reduce the financial benefits flowing to them, on the reasonable assumption that if the costs of serving tortious material grow roughly linearly with the number of users accessing that material, then without a viable source of revenue (typically advertising) such services will falter. Similarly, payment providers might be ordered to suspend transactions involving a notified website. These remedies are discussed in chapter 7.

---

[110] See James Grimmelmann, 'Some Skepticism about Search Neutrality' in Berin Szoka and Adam Marcus (eds), *The Next Digital Decade: Essays on the Future of the Internet* (2010) 435, 447. Cf Eric Goldman, 'Search Engine Bias and the Demise of Search Engine Utopianism' in ibid 461, 473.

[111] See, eg, DomainTools LLC, 'Recent Nameserver Activity: seizedservers.com' (5 May 2012) *DailyChanges* <http://www.dailychanges.com/seizedservers.com/>.

[112] See, in another context, Unspam Technologies Inc, 'About Project Honey Pot' (2012) <http://projecthoneypot.org/about_us.php>.

[113] See Dan Goodin, 'Unprecedented Domain Seizure Shutters 84,000 Sites' (18 February 2011) *The Register* <http://www.theregister.co.uk/2011/02/18/fed_domain_seizure_slammed/>; Kevin Murphy, 'ICE Domain Seizures Enter Second Phase' (20 April 2011) *Domain Incite* <http://domainincite.com/ice-domain-seizures-enter-second-phase/>.

[114] See Ben Sisario, 'Music Web Sites Dispute Legality of Their Closing' (*The New York Times*, 19 December 2010) <http://www.nytimes.com/2010/12/20/business/media/20music.html>.

[115] Margaret Grazzini, 'Four Rounds of ICE Domain Name Seizures and Related Controversies and Opposition' [2011] *Berkeley Technology Law Journal Bolt* <http://btlj.org/?p=917>.

(g) *Disconnection*

The most extreme form of enforcement is physical disconnection. This severs a defendant's machine from the network of its host or ISP, preventing it and any downstream clients from accessing the internet. This measure is discussed most commonly in the context of copyright infringement by individual subscribers,[116] but it has also arisen during warfare,[117] the suppression of uprisings by authoritarian regimes,[118] and the accidental severance of transoceanic cables.[119] Following the 2011 London riots, the government indicated that it would consider whether to develop a 'kill switch' which would disconnect social networks during times of civil unrest.[120] This proposal appears to have been abandoned, but disconnection continues to be discussed as an enforcement measure of last resort.[121] Some scholars argue in favour of disconnection for limited purposes such as cybersecurity[122] — a view endorsed by a House of Lords committee which recommended that ISPs be obligated to disconnect customers whose machines have been compromised.[123] Although disconnection is often analysed as a binary remedy, it is better understood as a spectrum of access restrictions ranging from outright disconnection at one extreme, to unfettered access at the other. Intermediate forms include: *play-penning*, in which a subscriber's access is restricted to a pre-approved whitelist of websites and services for a fixed period; *shaping*, in which the subscriber's connection speed is temporarily reduced; and *suspension*, in which access is terminated temporarily. Disconnection is not directly considered by this research, since it is usually targeted at end-users rather than intermediaries.

---

[116] See below chapter 5, § 3.1.

[117] See Matthew Broersma, 'Clinton Encourages Serbia Net Access' (14 May 1999) *ZDNet* <http://www.zdnet.com/news/clinton-encourages-serbia-net-access/102312>.

[118] See, eg, The Economist Newspaper Ltd, 'Reaching for the Kill Switch' (*The Economist*, 10 February 2011) <http://www.economist.com/node/18112043>.

[119] See, eg, BBC, 'Severed Cables Disrupt Internet' (31 January 2008) <http://news.bbc.co.uk/1/hi/technology/7218008.stm>.

[120] See, eg, Hansard, 'Public Disorder', House of Commons (11 August 2011, Mr David Cameron MP) col 1053.

[121] See, eg, Andrew Blum, 'Tunisia, Egypt, Miami: The Importance of Internet Choke Points' (28 January 2011) *The Atlantic* <http://theatlantic.com/technology/archive/2011/01/tunisia-egypt-miami-the-importance-of-internet-choke-points/70415/>.

[122] Jonathan Zittrain, *The Future of the Internet — And How to Stop It* (2008) 54, 166.

[123] House of Lords, Science and Technology Committee, *Personal Internet Security — Volume I: Report* (2007) 30–2.

4 Scope of research

Given the central role of intermediaries in electronic communications, their liability is of considerable interest to a society that values the continued freedom and utility of the internet. Like any other arena of human activity, the internet will inevitably house a population of wrongdoers and recidivists. Some wrongs are new phenomena made possible by digital networks, others merely the occurrence of familiar conduct in a new medium. As old doctrines are stretched and adapted to these environments, new patterns of activity must be translated into recognised categories of wrongdoing. Inevitably this process exerts pressure upon the margins of those categories and the classes of defendants who may be made to bear losses.

The purpose of this research is to understand *who* should be liable for internet wrongdoing and *how* rights should be enforced online. The essential puzzle is not *what* constitutes wrongdoing — such a question is a matter of applying existing doctrines in largely well-understood ways — but rather to identify when internet intermediaries may be held liable under secondary liability rules, and to evaluate whether existing remedies are fit for purpose. While comprehensive examination of all types of wrongdoing is well beyond the scope of this research, it can attempt a more modest inquiry; namely, to analyse the development and application of secondary liability rules for two torts (defamation and copyright) in English actions against intermediaries, and to consider whether new injunctive remedies (disclosure and non-facilitation) can be necessary and proportionate in those cases. This inquiry aims to contribute to scholars' understanding of secondary liability in English private law and to furnish an appreciation of how those rules regulate the conduct of intermediaries and their users. The following sections explain its scope in greater detail.

4.1 Research question

The subject matter of this research is the legal responsibility which electronic platforms and service providers bear for wrongdoing by third parties. The basis, margins and practical effects of existing secondary liability rules are poorly understood. They are known to be connected to overlapping notions of contributory, vicarious, derivative and accessory liability, but what, if anything, unites them, how they interrelate, and what values should guide their application, remain unresolved. Accordingly, this research seeks to answer three related questions:

> First, what is an internet intermediary and how do they relate to existing categories of secondary defendants in English private law?

> Second, when does English law hold such a party liable (a) to pay a monetary remedy; and (b) to give non-monetary remedies of disclosure or to prevent wrongdoing, where a person has been injured by defamation or copyright infringement facilitated by the intermediary's services?
>
> Third, how are those remedies to be balanced against the rights of innocent third parties in a fair and proportionate manner?

This research does not consider all forms of liability faced by intermediaries. Instead, it restricts itself to civil wrongdoing which is 'secondary' in the sense that it depends on a finding of at least *prima facie* liability of a third party. This encompasses both causative secondary wrongdoing[124] and certain primary wrongs, such as authorisation of copyright infringement, secondary publication of defamatory matter, and joint tortfeasance.

4.2 Relationship to existing scholarship

Existing scholarship touches on but does not directly resolve these issues. As discussed above, previous scholars have focussed their attention on five related puzzles: first, the scope of the rights which ought to be protected by each tort, corresponding to boundaries of primary liability; second, how new communications technologies are and should be regulated, typically from the perspectives of law and economics, political theory and human rights; third, the evolution of secondary liability in particular fields, especially copyright; fourth, secondary liability rules in offline contexts, such as economic torts; and fifth, intermediary liability in other jurisdictions, especially the United States and Australia.

Although some scholars have considered the liability of English intermediaries, this research builds on those contributions in four ways. First, it discusses the historical foundations and development of secondary liability rules, providing a more detailed context within which to assess their expansion. Second, it offers a systematic comparison of secondary liability rules — in particular the principles governing non-monetary remedies — and their role in regulating internet technologies. While their importance is generally accepted, no attempt has been made to rationalise or map the boundaries or underlying basis of intermediaries' liability in England. Third, it discusses a growing corpus of recent case law which has not been analysed elsewhere. Finally, it adopts a structure and taxonomy which better reflect the technical attributes of internet intermediaries and permit more accurate analysis of their liability.

---

[124] See below chapter 3, § 1.1.

4.3 Exclusions

Five important topics are excluded from this research entirely. This section identifies and defends those exclusions.

(a) *Primary and relational liability*

This research does not consider intermediaries' primary liability for their own acts of defamation or copyright infringement. This means to exclude liability arising exclusively from the conduct of intermediaries or from parties in recognised relationships with them (such as agents or employees). Liability is primary where, for example, an employee of Google herself authors and publishes a defamatory article or downloads an infringing sound recording. These scenarios are uninteresting because they raise familiar questions about a party's liability for her own acts or omissions (or vicarious liability for those of employees). Instead, this research is directed at intermediaries' *secondary* liability — that is, liability deriving in some sense from tortious content created or disseminated by third parties. This distinction is explained further in chapter 3.

(b) *Types of wrongdoing*

This research is limited to liability arising under English doctrines of defamation and copyright infringement. These wrongs were chosen because they present both the most important doctrinal questions and the most developed bodies of jurisprudence. They provide two contrasting examples of secondary liability circumscribed by: (1) a primary limiting criterion ('publication' in defamation law and 'authorisation' in copyright law); (2) common connecting factors (such as principles of joint tortfeasorship); (3) safe-harbours and limitations; and (4) *sui generis* enforcement mechanisms. At a more practical level, confinement is necessary to permit space for sufficient depth of analysis. Because each wrong protects substantially different interests and has a large body of associated scholarship, it is necessary to focus exclusively on the principles that determine their outermost boundaries of liability.

Three exclusions warrant particular explanation. First, trade mark claims are excluded because they tend to implicate limited classes of intermediaries (principally search engines and online marketplaces) and in England do not rely upon a formal doctrine of secondary liability (though they do employ limiting criteria such as 'use' and connecting factors including joint tortfeasorship). Second, contractual claims are excluded because they are, by definition, examples of primary liability; further, they are determinable by conventional principles of formation and interpretation. Third, a range of consumer protection and trade practices statutes impose liability

upon intermediaries. However, their effect on intermediaries tends to be incidental and their objects penal rather than compensatory.

(c) *Criminal liability*

This research is concerned only with the civil liability of intermediaries. Criminal liability is excluded because doctrines of joint criminal responsibility raise different conceptual, practical and historical issues. Some scholars have argued that identical principles of secondary liability should apply; this literature is dealt with briefly in chapter 3.

(d) *Liability under foreign law*

For reasons of scope, the research considers only the position in England under English and EU law. This is justified because: (1) most existing literature concerns the position in other jurisdictions; (2) the cross-border nature of internet wrongs, flexible localisation rules and broad jurisdiction mean that local proceedings will often be available, even if intermediaries are domiciled elsewhere; (3) significant intermediary businesses already operate or have a presence within England; and (4) future regional harmonisation of secondary liability within the EU will be informed by and interpreted using current domestic rules. Non-EU decisions — principally those of American, Canadian and Australian courts — are considered only to the extent they shed light on the likely English position in the absence of reported decisions.

(e) *Theories of remedies and regulation*

This research does not comment on whether the internet is a 'powerful force for good'[125] or a pernicious platform of vilification and abuse. Nor does this research engage in theoretical debates about regulation, innovation, human rights, the choice between property and liability rules, the nature of rights, wrongs and remedies, or the justifications for tortious liability. Although the phrase 'internet freedoms' is used in part 3 to denote a bundle of rights and freedoms enjoyed by internet users — including freedom of expression, commerce and association, and the rights to private life, data protection, correspondence and a fair trial — this thesis does not seek to make any normative argument about the desirability or scope of these rights. Instead, it proceeds from the starting point that courts should wherever possible act compatibly with human rights when

[125] House of Lords, *Personal Security*, above n 123, 7.

determining and applying intermediary liability rules. It offers no contribution to wider debates about primary legal norms.

5 Methodology

Two methodological choices warrant comment. The first addresses the charge that the chapters which follow are excessively formalist. This introduction has sought to situate intermediary liability within a wider context of internet regulation and the 'virtuous self-amplifying circle' of innovation.[126] That choice reflects the recognition by realist and social scholars that a full appreciation of liability rules requires us to study their complex interplay with other regulatory forces.[127] However, this research cannot fully analyse the important roles of trade policy,[128] European federalism,[129] social practices, 'code',[130] market forces and cultural differences which shape the development and application of legal rules. Although partially interdisciplinary in its attempts to draw on technological and historical insights, this research is open to the criticism of 'legal centralis[m]'.[131] It necessarily furnishes an incomplete understanding of the terrain.

Nevertheless, it is suggested that formalism offers a useful approach to the problem for three reasons. First, irrespective of wider influences, English courts continue to apply (or purport to apply) extant legal rules to resolve disputes, with little consideration of wider policy questions beyond the extent necessary for, say, statutory interpretation or judicial review. Despite uncertainty, lawyers must advise claimants and intermediaries as to their likely rights and liabilities under English law. It is therefore important to begin with an accurate descriptive account of those principles as practised by our legal institutions. Second, it is frequently suggested that particular information torts are out of date or strike the wrong balance between freedom of expression and other rights. To determine whether these criticisms have merit, it is necessary to understand the boundaries of those wrongs and how they have evolved. A doctrinal methodology lends itself well to critical analysis of this nature, being characterised by an 'expository flavour'

---

126 Kevin Kelly, *What Technology Wants* (2010) 308.

127 See Lawrence Lessig, 'The New Chicago School' (1998) 27 *Journal of Legal Studies* 661.

128 See Graeme Dinwoodie and Rochelle Dreyfuss, 'TRIPS and the Dynamics of Intellectual Property Lawmaking' (2004) 36 *Case Western Reserve Journal of International Law* 95, 112.

129 See Rizzuto, above n 70, 77–8.

130 Lessig, above n 26, 86–9.

131 Robert Ellickson, *Order without Law: How Neighbors Settle Disputes* (1991) 137.

and 'focus on written sources of law'.[132] Finally, doctrinal analysis is a necessary preparation for scholars to appreciate the complex and bidirectional relationship between the 'soft' technology of law and the 'hard' technology of the internet.[133] Rather than make vague generalisations about internet regulation, this research will consider specific instances of liability and directly analyse how they have come about and whether they encourage desirable properties of technology and human behaviour.

The second defence concerns underlying regulatory assumptions. This research does not proceed from a starting point of 'exceptionalism'. That is, it does not argue that the internetworked environment is intrinsically new or different in such a way that requires new legal norms. To the contrary, the same classes of wrongs and harms persist online. These wrongs may differ in method and degree, but they do not necessitate new primary rules unless they fundamentally alter the relationships between claimants and tortfeasors. However, the nature of the internet does make intermediary-based regulatory strategies more effective than in offline settings.[134] As described in section 1, intermediaries *must* be used to effect wrongdoing — unlike the real world, where individuals can interact directly — and tortfeasors can act anonymously with far greater ease unless monitored by intermediaries (who possess unique capacity to do so). Although these differences may affect policymakers' choice of *enforcement* mechanism, this research assumes that incremental development of the law by analogy with established principles remains the surest guide to optimal rule-making in individual cases. This process of adaptation is not without design choices which confront judges, and which should be resolved to promote values intrinsic in primary legal norms, such as the protection of fundamental rights and the encouragement of innovation. Beyond noting those choices, this research does not seek to advance any particular set of norms as true.

Having situated the subject matter of this research and defended its structure and methodology, chapter 2 defines and classifies 'internet intermediaries' according to their technical functions and position in an architectural taxonomy.

---

[132] Arlie Loughnan and Rita Shackel, 'The Travails of Postgraduate Research in Law' (2009) 19 *Legal Education Review* 99, 107.

[133] See Kelly, above n 126, 349–50.

[134] See Mann and Belzley, above n 52, 239, 267–8.

2
The Nature of Internet Intermediaries

Chapter 1 provided a general introduction to this research by reference to the social, economic and remedial roles of internet intermediaries. This chapter further develops these actors as a legal category and situates their conduct within the technical architecture of the internet. Relatively few scholars have considered how network architecture informs the development and application of secondary liability rules to intermediaries.[1] Building upon insights from computer scientists and economists,[2] this chapter aims to reconceptualise the internet intermediary as a functional

[1] See especially Kevin Werbach, 'The Network Utility' (2011) 60 *Duke Law Journal* 1761; de Beer and Clemmer, above n 49 (ch 1).

[2] See, eg, Benkler, above n 19 (ch 1); David Reed et al, 'Active Networking and End-to-End Arguments' [1998] *IEEE Network* 69.

actor in a layered, modular network system. A layered definition enables us to understand their different contributions to wrongdoing and to explain why some intermediaries are legally responsible for harm while others are excused as neutral conduits. This chapter does not advocate a position of technological determinism — it does not assume liability rules should mould to the contours of the technology they regulate[3] — but instead argues that design choices inherent in the internet's structure are relevant to liability rules in three ways: first, in supplying a vocabulary to describe defendants' conduct (the descriptive function); second, in determining what measures are reasonably available to intermediaries tasked with regulating misconduct (the possible conduct function); and second, in choosing between alternative liability standards in ways that preserve desirable attributes of internet platforms (the normative function).

Section 1 identifies several attributes of intermediaries by induction from four examples of offline intermediaries: (1) a causal relationship to harm; (2) a conduit function; (3) capacity to enforce third parties' rights; and (4) proxy regulation. Section 2 briefly examines existing definitions of internet intermediaries, which it observes are imprecise or incomplete. Section 3 explains basic principles of internet architecture and describes the position of internet intermediaries within the broader structure of electronic communications. Finally, section 4 proposes a network layer taxonomy to classify intermediaries by their technical function.

1 The nature of an intermediary

1.1 Offline intermediaries

This section briefly identifies four classes of entity which can act as intermediaries in contexts unrelated to the internet. Considering the treatment of 'offline' intermediaries is useful for both comparative and definitional purposes. It is suggested that offline and online intermediaries share three common features: first, they can be causally significant but insufficient causes of harm to third parties; second, their *prima facie* liability is generally not determined by universal principles of secondary responsibility but by the application of context-specific doctrines and remedies; and third, their presumptive liability is often limited for reasons of public policy. The following

[3] Cf Thomas Folsom, 'Toward Non-Neutral Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses' (2009) 3 *Akron Intellectual Property Journal* 45, 73–4, 98–9.

examples are not exhaustive; doubtless, many other instances of offline intermediaries could be identified, including financial brokers, auctioneers, and marketplaces.[4]

(a) *Postal services*

The Post Office is the archetypal intermediary. It is, in effect, a network for information sent by means of packages sent by senders to recipients. Occasionally those packages cause harm (as in the case of a letter-bomb, a defamatory pamphlet or a counterfeit medicament) but, intuitively, we know that it is not the Post Office which is responsible for this harm, even though it may have been one cause of it by carrying the relevant article. Instead, we say that the wrongdoer is the sender, and the Post Office merely their innocent 'agent' or a conduit for the material.[5] The Post Office is clearly an insufficient cause of harm, since without its sender the package would never have arrived,[6] but it is necessary to the primary event which occurred (delivery). The Post Office might have been able to prevent the harm, albeit at significant cost, by inspecting and approving each package during transit, but we do not expect that it will do so.[7]

The conduit status of postal services is codified by statute. Section 29(1) of the *Post Office Act 1969* (UK) immunised the Post Office and its agents from liability 'for anything done or omitted to be done in relation to anything in the post', while s 29(2) extended the immunity to loss or damage arising during the carriage of mail.[8] Section 90 of the *Postal Services Act 2000* (UK) carries forward these exemptions to the modern privatised entities, subject to limited exceptions.[9] Interpreting analogous legislation, *Triefus & Co Ltd v Post Office* held that the postal authorities had no liability to the sender for mail that was stolen by a third party.[10] The principle of immunity is long-standing: in 1699, *Lane v Cotton* exonerated the post-master general from liability for a stolen cheque.[11] Such an office was considered 'so extensive, and requires such a number of servants, &c speed in conveyance, journeys by day and night [that] it resembles the case of piracy,

---

4 See Case C-324/09, *L'Oréal SA v eBay International AG* [2011] ETMR 52, 1004 (Advocate–General Jääskinen) ('*eBay (CJEU)*').

5 See, eg, Edwards and Waelde, above n 42 (ch 1), 24; Jim Harper, 'Against ISP Liability' [2005] *Regulation* 31.

6 The Post Office (or its delegates) might also send mail on behalf of itself. When it does so, the Post Office is acting as a primary party: see below chapter 3, § 1.1.

7 See, eg, *United States Constitution* amend IV; *Ex parte Jackson*, 96 US 727, 733 (1877).

8 See Christopher Walton (ed), *Charlesworth & Percy on Negligence* (12th ed, 2010) [3-27].

9 See *Postal Services Act 2000* (UK) ss 89, 91 (which permit liability for loss arising due to any 'wrongful act' or default by the service provider or their delegate).

10 [1957] 2 QB 352, 368 (Parker LJ).

11 (1701) 1 Ld Raym 646; 91 ER 1332.

which is *damnum fatale*.'[12] To similar effect, in *Whitfield v Lord Lé Despencer* Lord Mansfield concluded that any action on the case lies against 'the party really offending' and not the post-master, who is liable only for his *own* fault.[13] In the 19th century, the telegraph department of the Post Office was treated similarly.[14] In response to the absence of intermediary liability rules, correspondents adopted self-help measures — such as cutting bills and notes into multiple parts sent on successive days — to protect themselves from fraud.[15]

During industrial action in the late 1970s, the Court of Appeal held that the principle of immunity meant it had no jurisdiction to grant an injunction against employees of the Post Office who were detaining the claimants' mail in protest.[16] Lord Denning MR said of s 29 simply: 'It is very wide. It is "any loss or damage suffered by any person."'[17] Because this section meant there was no action in conversion against the employees, no mandatory injunction could issue which required them to forward the claimants' mail. Even if the Court could grant such an injunction, it would decline to exercise its discretion because that would require the postal employees to 'discriminate' between recipients. All members of the Court were clearly concerned to ensure that the Post Office remain a content-neutral intermediary; intervening so as to require its officers to differentiate between mail would 'create such a bad precedent — with so much danger for the future'.[18] Again, losses were left to lie where they fell.

(b) *Carriers*

Airlines, cargo ships, couriers and other carriers act as intermediaries when they transmit property belonging to a third party consignor from one location to another. Unlike the Post Office, they owe manifold contractual and non-contractual duties as bailees and common carriers, and enjoy no broad statutory immunity. These duties are primary in the sense that they are undertaken by the carrier's voluntary acceptance of goods — or implied by statute[19] — and breached when the carrier fails to protect the bailed goods. It is clear that these duties can also be breached because of consequences brought about by the acts of third parties — for example, if a

---

12 Ibid 648; 1333.

13 (1778) 2 Cowp 754, 764–6; 98 ER 1344, 1349.

14 See *Telegraph Act 1868* (UK) s 2; cf *Telegraph Act 1863* (UK) s 42; *Bainbridge v Postmaster–General* [1906] 1 KB 178, 187–9 (Collins MR), 194 (Mathew LJ).

15 Ibid 766; 1349 (Lord Mansfield).

16 *Harold Stephen & Co Ltd v The Post Office* [1977] 1 WLR 1172.

17 Ibid 1177 (Lord Denning MR).

18 Ibid 1178–9 (Lord Denning MR), 1179 (Browne LJ), 1180 (Lane LJ).

19 See, eg, *Carriage of Goods by Sea Act 1971* (UK).

thief misappropriates bailed property from a furrier,[20] airline,[21] shipowner[22] or railway operator.[23] The thief may be an independent cause of another wrong (theft), but the carrier is primarily liable for failure of the bailment. This is primary liability for breach of a primary duty.[24]

Liabilities for the carriage *per se* do not concern carriers in their capacity as intermediaries but rather as agents who are engaged for the express purpose of securely bringing goods to a destination; it is therefore unsurprising that they are held strictly liable for damage to those goods. Further, there exist statutory causes of action which impose absolute liability upon railway operators,[25] airlines[26] and common carriers for damage to goods. These liabilities are, of course, subject to various limitations and exclusions which reflect public policy, such as the need to ensure the economic viability of supplying carriage services.[27] For example, railway operators are exempted from liability for nuisance and certain related harms.[28] Another way of thinking about carriers' liability is that they may be liable to the consignor and consignee, but are generally not liable to third parties, absent some special relationship.

On the other hand, a bailee is rarely liable for wrongs carried out by means of transporting the goods, but which fall outside the scope of the bailment — such as losses caused by delivering defamatory goods, transporting goods which infringe a patent, or detaining goods that belong to another. Although there are few clear statements of principle, this appears to be because the originating wrongdoer is the consignor rather than the bailee. In *Morton–Norwich Products Inc v Intercen Ltd*, the defendants imported patented chemical compounds into the United Kingdom.[29] The carriage was effected by British United Airways, which took the goods from Rotterdam to Gatwick. Although the airline was acting as agent for the consignee, there was no suggestion that it was liable for the resulting patent infringement.[30] The question appears to have been

---

[20] See *Morris v C W Martin & Sons Ltd* [1966] 1 QB 716, 729 (Lord Denning MR), 731 (Diplock LJ), 737 (Salmon LJ).

[21] See *Moukataff v British Overseas Airways Corp* [1967] 1 Lloyd's Rep 396.

[22] See *Elder, Dempster and Company Ltd v Paterson, Zochonis and Company Ltd* [1924] AC 522, 535–6 (Viscount Finlay).

[23] See *HSBC Rail (UK) Ltd v Network Rail Infrastructure Ltd* [2006] 1 WLR 643, 651–2 (Longmore LJ) (Lloyd LJ and Morritt C agreeing).

[24] See Robert Stevens, *Torts and Rights* (2007) 120. See below chapter 3, § 1.1(a).

[25] *Railway and Canal Traffic Act 1854* (UK) s 7 (repealed).

[26] *Carriage by Air Act 1961* (UK) sch 1, arts 17–22, 27, 30(3); *American Express Co v British Airways Board* [1983] 1 WLR 701, 708 (Lloyd J).

[27] Eg, the *Post Office Act* applies to airlines acting in the capacity of a postal carrier: ibid 708 (Lloyd J). See also *Carriers Act 1830* (UK) s 1 (limiting liability).

[28] *Railways Act 1993* (UK) s 122(3) (excluding liability 'in any civil proceedings' in nuisance or 'in respect of the escape of things from land'). See also s 123 (deeming railways not to be common carriers).

[29] [1978] RPC 501 ('*Intercen*'). See further chapter 6, § 2 in relation to *Norwich Pharmacal* orders.

[30] Ibid 506–7 (Prescott, in argument), 509 (Turner QC, in argument) ('it was only a carrier … and a mere carrier does not infringe'), 518 (Graham J).

resolved as a matter of principle: simply possessing, transporting[31] or warehousing an invention is not necessarily 'use' of it by the carrier.[32] Liability is thus fixed according to the boundaries of individual torts.[33]

(c) *Highway and canal authorities*

Road traffic controllers, tollway operators, canal-ways and other highway authorities owe various duties to their users and owners of neighbouring properties.[34] Many of these duties are public in nature and do not create rights in private parties.[35] To the extent they do, these statutory duties are not absolute. Thus, the owner or operator of a road is not normally liable for the negligent conduct of road users, whose acts are their own: a mere omission by the highway operator will not create liability without 'some special justification' or a specific statutory duty.[36] The fact that the road may be a necessary cause of the third party's wrongdoing is insufficient because the operator acts as a pure intermediary for all traffic.

(d) *Utilities*

Whereas the Post Office is a conduit for printed messages and goods, utilities are conduits for energy and other natural resources. While they owe various obligations in their primary capacity as *energy suppliers* — to ensure continuity of service, safety of supply and storage[37] — they are not liable for wrongs committed by customers using the electricity they provide, though little authority exists on the point.[38] Gas and nuclear power producers are strictly liable for loss caused by the escape of their hazardous materials,[39] but not simply because energy is used tortiously. They supply essential preconditions for engaging in many species of wrongdoing (as do automobile service stations, vendors of firearms and almost any other merchant) without possessing control over how their resources are used by customers.

---

31 *Pfizer Corporation v Ministry of Health* [1965] AC 512, 571–2 (Lord Wilberforce).

32 *Badische Anilin und Soda Fabrik v Basle Chemical Works (Bindschedler)* [1898] AC 200, 208–9 (Lord Halsbury LC) (Lord MacNaghten, Lord Morris, Lord Shand and Lord Davey agreeing).

33 See, eg, *Wilson v Lombank* [1963] 1 WLR 1294 (trespass to goods).

34 See, eg, *Highways Act 1980* (UK) ss 41(1), 79(1); *Gorringe v Calderdale Metropolitan Borough Council* [2004] 1 WLR 1057 (duty to maintain the highway).

35 Ibid 1070 (Lord Hoffmann), 1078–9 (Lord Scott).

36 *Stovin v Wise* [1996] AC 923, 929–30 (Lord Nicholls) (dissenting), 957–8 (Lord Hoffmann).

37 See, eg, *Water Industry Act 1991* (UK) s 209 (imposing strict liability for loss caused by water escaping from a pipe); *Merchant Shipping Act 1995* (UK) (imposing strict liability for escape of hazardous chemicals from ships).

38 See, eg, *iiNet*, [400] (Cowdroy J); [2011] FCAFC 23, [384] (Jagot J).

39 *Gas Act 1965* (UK) s 14(1); *Nuclear Installations Act 1965* (UK) s 7 (imposing strict liability for damage caused by nuclear matter or ionising radiation);

1.2 Attributes of intermediaries

Certain common features emerge from the foregoing discussion, from which it is possible to synthesise a better working definition of an intermediary. This section argues that intermediaries are united by the attribute that a third party, B, can utilise their services or status to cause loss to C, where the combination of B's acts and the assistance of A, the intermediary, is sufficient to cause the loss, but A's assistance alone is insufficient. This role can be described in several ways, which together distinguish intermediaries from other classes of defendant.

(a) *Intermediary as cause*

Where intermediaries have a causal relationship with harm, it is usually[40] by contributing to the performance of acts carried out by another, as where A (the intermediary) tells B to inflict harm on C. This may be by inventing or providing B with an essential tool, supplying necessary persuasion or encouragement to B, or failing to do something which would have made it impossible for B to act. The intermediary is a necessary[41] but insufficient cause of the harm: without B, the event causing harm would not have occurred, despite A's conduct. An intermediary is *never* a sufficient cause of the harm to C: that is, A does not itself perform the acts which inflict harm on C. In the obverse case — where A provides no contribution to B, but B still inflicts harm on C — A is not a causally relevant party; instead we say that B is the sole cause of C's injury and, absent some special duty to control B or protect C, no liability can be attributed to A. Thus, we can conclude that a person *might* be acting as an intermediary when she is a necessary but insufficient cause of harm to another, and where the combination of the intermediary and any third party wrongdoers are together necessary and sufficient causes of the harm. Of course, factual causation supplies an incomplete explanation: simply causing harm is not conclusive of liability. Many other factors — including mental state, the nature of the harm, the legal classification of B's conduct, the intervention of subsequent wrongdoers, and the availability of liability-limiting defences — are relevant. Nevertheless, almost all intermediaries are causes of harm and the nature of this causal relationship is an important feature of any discussion about their liability.

---

[40] See further chapter 3, § 1.1 for discussion of causal relationships with wrongdoing. Although an intermediary can itself inflict harm on C, such a fact pattern is properly described as primary conduct and does not concern us here.

[41] 'Necessary' is here used to mean a factor which is involved in the occurrence of the event which did occur: see Jane Stapleton, 'Choosing What we Mean by "Causation" in the Law' (2008) 73 *Missouri Law Review* 433, 444–6.

(b) *Intermediary as conduit*

In its most general and literal sense, an intermediary is '[o]ne who acts between others; an intermediate agent; a go-between middleman',[42] or an entity 'acting between persons', a 'means'.[43] These definitions suggest another attribute of intermediaries: that they exist only between two other entities or events such as to connect them in a defined way. Who are these 'others'? In the context of online wrongdoing, an intermediary assists the primary wrongdoer, to whom it typically supplies information services. It also has a causal connection to any downstream parties who suffer loss caused by the actions of the primary wrongdoer. Thus, on one side sits a wrongdoer and, on the other, a network of users and victims; connected along a causal chain mediated, at some point, by an intermediary.

To say that the intermediate party is an *agent* (in the colloquial sense) or *middleman* is to describe a collateral entity whose actions are not products of its own freewill but rather the conveyance of another party's choices. This can occur in two ways. First, the intermediary's act or omission may occur prior to the wrongdoer's conduct, as an essential precondition by providing the means, identifying the victim or priming the wrongdoer. In this situation, the intermediary is 'arming' the wrongdoer, making the harm possible without participating in it. In the second case, the intermediary is inserted into the middle of the causal chain: propagating a harmful action without arresting its progress so that its harmful effects are felt by others or magnified. Multiple intermediating parties can of course be interposed between the end links in the chain. However, not all intermediaries act as conduits in this strict sense: many will choose to intervene in a course of conduct in clearly-defined and influential ways.

Courts often invoke the metaphor of a 'conduit pipe'. In *Weld-Blundell v Stephens*, for example, Lord Sumner described the question of whether a third party's intervention constituted a *novus actus interveniens* as being whether it was

> no mere conduit pipe through which consequences flow from [defendant to claimant], no mere part of a transmission gear set in motion by [the defendant][44]

Metaphors can be misleading. Browne LJ cautioned against the use of 'such metaphorical (and I think unhelpful) phrases as "conduit pipe" (or "mere conduit pipe")' in the context of conversion.[45] Nevertheless, the metaphor shows that intermediaries can act as both *transmitting* and *arming*

---

[42] *Oxford English Dictionary* (2nd ed, 1989) (entry for 'intermediary', *noun*), (B)(1).

[43] Ibid (B)(2).

[44] [1920] AC 956, 986 (Lord Sumner).

[45] *R H Willis and Son v British Car Auctions Ltd* [1978] 1 WLR 438, 444 (Browne LJ).

parties while another wrongdoer remains the ultimate source of harm. Some intermediaries, at least, are like rivers: 'mere' passive conduits which care not what flotsam they carry into the harbour. The assumption underlying this metaphor is a degree of involuntariness, removing many of the normative justifications for liability.

(c) *Intermediary as enforcer*

Just as they can cause harm by connecting wrongdoers and victims, intermediaries are frequently in a position to prevent harm by withholding support from wrongdoers or detecting and policing misconduct before it causes loss.[46] In other words, intermediaries tend to be effective enforcers because they can sever the causal chain — diverting the course of the river — before an inchoate wrong has been completed. This *ex ante* enforcement may be preferable to *ex post* liability rules if the costs of pre-emptive action are less than the costs of shifting the resulting losses from victim to wrongdoer.

Ex ante enforcement by intermediaries may be more efficient for three reasons. First, increased collateral enforcement can deter primary wrongdoers by increasing the maximum expected penalty. Most internet wrongdoing involves highly distributed but minor misconduct where the costs of enforcement are likely to outweigh the amount recoverable by an enforcer against each individual wrongdoer.[47] This reduces the odds of detection and punishment, which correspondingly diminishes the expected cost of misconduct. By making detection more likely, intermediaries reduce the expected value of misconduct to wrongdoers. Second, intermediaries may be able to interdict misconduct more cheaply than victims, regulators or market-based enforcers because they possess better information about the wrongdoer or greater technical capacity to detect wrongdoing. Finally, inadequate incentives may exist for private parties to proceed against wrongdoers. These rationales are explored further in chapter 3.

(d) *Intermediary as regulator*

Intermediaries are both subjects of regulation by law and regulators of their users' behaviour. As aggregators and custodians of information, they are uniquely qualified to define and enforce policies and rules within their domains. While this is particularly true of internet intermediaries,

---

[46] Reinier Kraakman, 'Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy' (1986) 2 *Journal of Law, Economics, and Organization* 53, 54, fn 3.

[47] Ibid 92.

which can define code-based limits, it also defines many offline intermediaries, such as broadcasters, carriers and couriers. Because intermediaries control the flow of information in these relationships, they function as 'points of control'[48] over knowledge, access and culture. Intermediaries can also be appointed as quasi-public regulators. This strategy is particularly attractive where it is unfeasible for the state to regulate individual speakers directly. Kreimer has identified such intermediaries as 'proxy censors'[49] whose control over information makes them private regulators of a wide range of human behaviour.

2 Defining internet intermediaries

The subject matter of this research is the 'internet intermediary'. Like other abstract words which are capable of application to a wide range of circumstances, 'intermediary' lacks an obvious correspondence to tangible facts or human experiences.[50] It is used to describe many entities which seem to share little in common. The internet intermediary is an unhappy abstraction — a *genus* whose many members' common features have never been systemically identified. These difficulties partly explain its tendency to elude precise definition. They are compounded by the addition of imperfect synonyms — 'mere conduits', 'secondary',[51] 'accessory'[52] and 'participatory'[53] parties — and the substitution of taxonomically indistinct sub-categories, such as 'internet service providers',[54] 'facilitators',[55] 'enablers',[56] 'vicarious infringers',[57] and 'joint tortfeasors'.[58]

---

48 Jonathan Zittrain, 'Internet Points of Control' (2003) 44 *Boston College Law Review* 653, 688.

49 Seth Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155 *University of Pennsylvania Law Review* 11, 17.

50 See H L A Hart, 'Definition and Theory in Jurisprudence' (1954) 70 *Law Quarterly Review* 37, 38–9.

51 See Patrick Atiyah, *Vicarious Liability in the Law of Torts* (1967) 289; Philip Sales, 'The Tort of Conspiracy and Civil Secondary Liability' (1990) 49 *Cambridge Law Journal* 491.

52 See Paul Davies, 'Accessory Liability: Protecting Intellectual Property Rights' [2011] 4 *Intellectual Property Quarterly* 390, 396.

53 See Eva Lomnicka, '"Knowingly Concerned"? Participatory Liability to Regulators' (2000) 21 *Company Lawyer* 120, 121.

54 See World Intellectual Property Organization, Standing Committee on Copyright and Related Rights (4–8 November 2002) SCCR/8/2, 2.

55 See Hamdani, above n 31 (ch 1), fn 2, 902–3; Lichtman and Posner, above n 45, 227.

56 See *Communications Decency Act 1996* (US) 47 USC § 230(f); Decree No 468 of 18 May 2006, *Regulation on Protection of the Right of Communication via Information Networks* (CN) art 22.

57 See Alfred Yen, '*Sony*, Tort Doctrines, and the Puzzle of Peer-to-Peer' (2004) 55 *Case Western Reserve Law Review* 815, 820.

58 See Dennis Lievens, 'eBay's Accessory Liability for Counterfeiting — Why Joint Tort Liability Just Doesn't Cut the Mustard' (2011) 42 *International Review of Intellectual Property and Competition Law* 506, 508–9.

Attempts to define the concept exhaustively are likely to encounter difficulty for several reasons. First, an intermediary is a formless and shifting analytical concept whose precise meaning depends on context — online or offline, financial or legal, vertical or horizontal — and which expresses a conclusion about the nature of a relationship between parties. Second, scholars and legislators use different terms to achieve particular rhetorical effects. Some descriptions suggest inherent neutrality ('conduit' or 'pipe', for example), while others ('gatekeeper', 'accessory party' or 'platform operator') suggest active participation. As MacCarthy notes, labels are chosen by 'stakeholders with specific aims, and carefully massaged so as to have particular resonance for particular audiences'.[59] This is particularly true of internet intermediaries, which are variously described in ways that reflect the competing ideologies of civil libertarians, rights-holders, regulators and technologists.[60] Third, the concept's boundaries and membership are constantly shifting. Amidst constant technological change, any fixed definition risks being either unhelpfully abstract or prematurely redundant. Bearing in mind these difficulties, this section considers existing definitions in legislation, case law and secondary materials. It argues that these definitions are inadequate and often contradictory, but contribute several useful attributes.

2.1 Legislation

(a) *E-Commerce Regulations*

The main legal definition of an internet intermediary is contained in the *Electronic Commerce (EC Directive) Regulations 2002* (UK) ('*E-Commerce Regulations*'), which transpose the provisions of the E-Commerce Directive[61] into United Kingdom law. The *Regulations* define the concept of an 'information society service provider', a subclass of internet intermediary that may invoke statutory safe harbours, as follows:[62]

> any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[63]

---

[59] Mark MacCarthy, 'What Payment Intermediaries Are Doing about Online Liability and Why it Matters' (2010) 25 *Berkeley Technology Law Journal* 1037, 1038.

[60] The choice of the term 'intermediary' is also open to this criticism, though it is suggested that the term is more neutral than the alternatives.

[61] Directive 2000/31/EC [2000] OJ L 178/1 ('E-Commerce Directive').

[62] The E-Commerce Directive, in turn, incorporates the definition of 'services' from article 1(2) of Directive 98/34/EC [1998] OJ L 204/37, as amended by Directive 98/48/EC [1998] OJ L 217/18 ('Technical Standards Directive').

[63] Technical Standards Directive art 1(2) (definition of 'service').

Three elements merit attention. First, subject to the requirement that services are delivered electronically and remotely, the definition is technology-neutral. Almost any 'economic activity' occurring via the internet is included, by any natural or legal person.[64] Second, data must be requested by a user of the services; in other words, the service provider cannot be a broadcaster that determines when and what transmissions occur. Third, the service must be provided commercially, even if remuneration is not supplied by the immediate recipient. This excludes personal email communications between individuals,[65] but is otherwise interpreted broadly; the activity must simply form part of some profit-making or subsidised enterprise.[66]

The *Regulations* and Directive appear to treat 'information society service provider' as a subset of a wider category of services. For example, section 4 of the Directive is entitled 'Liability of intermediary service providers' and sets out four safe harbours which apply to qualifying information society services.[67] In the *Regulations*, section titles are omitted but the explanatory note confirms that the defences are intended to shield 'intermediary service providers'. The definition is narrower because it only applies to *economic operators* and not non-commercial intermediaries (such as private correspondents), who may in other respects supply relevant services. However, recital (4) of the Directive refers to 'service providers acting as intermediaries', in that their activities are 'of a mere technical, automatic and passive nature'.[68] These requirements reflect the traditional view of an intermediary as conduit facilitator. Four examples suffice to illustrate the boundaries of this definition.

(i) *Website operators*

Websites supported by advertising, sponsorship or other commercial arrangements — or which themselves promote commercial services — are likely to be relevant service providers. Even personal websites, such as blogs and discussion fora, which have no profit motive or revenue model, may qualify for protection: in *Kaschke v Gray*, Stalden J held that the proprietor of a political website which hosted user-generated content was unquestionably providing an information society service.[69]

---

64 E-Commerce Directive recital (18), art 2(b).

65 E-Commerce Directive recital (18).

66 E-Commerce Directive recital (20).

67 E-Commerce Directive arts 12–15.

68 E-Commerce Directive recital (42).

69 [2010] EWHC 690 (QB), [43] (Stalden J) ('*Kaschke*').

(ii) *Hosts*

Almost all hosts of internet data would qualify for protection, on the basis that these are services for which a fee is usually charged. Even free hosting services — such as image or video storage platforms, and incidental storage provided as part of a social network — would satisfy the definition if supported by advertising or other commercial activity; almost all of these services store data electronically at their users' requests without knowledge or control.

(iii) *ISPs*

For similar reasons, commercial ISPs are considered service providers. Their equipment fetches, routes and transmits data at the direction of subscribers. In *Bunt v Tilley*, for example, Eady J held that it was 'clear' the defendant ISPs fell within the definition.[70] By analogy, so would mobile network operators. Whether the providers of free wireless hot-spots in coffee shops or hotels supply an information service is more doubtful; although often attached to a related retail business, the *economic* component of the activity is not supplied 'at a distance' — so too for internet cafés.

(iv) *Search engines*

To the extent they store, process and communicate user-created content in their indices and search results, advertising-supported gateways are likely to be service providers. In *DesignTechnica*, Eady J concluded that the *Regulations* 'are apt to cover those providing search engine services'.[71] His Lordship considered it 'a distortion of language' to describe advertising revenue as evidence that search engines were normally operated 'for remuneration'. Despite this, the Court reluctantly adopted the extended definition embraced by recital (18) of the Directive, which lists among its examples 'those providing tools for search, access and retrieval of data'. However, Eady J cautioned that this conclusion was not free from doubt. Several other member states have expressly extended the definition to search engines — a practice encouraged by the Commission and desirable for legal certainty.[72]

---

[70] *Tilley*, 1253 (Eady J).

[71] *DesignTechnica*, [84] (Eady J).

[72] European Commission, *First Report on the Directive on Electronic Commerce* (2003) 13.

(b) *Other domestic legislation*

Various other domestic statutes incorporate but add little to the definition set out in the *E-Commerce Regulations*.[73] For example, s 97A of the *Copyright, Designs and Patents Act 1988* (UK) ('*Copyright Act*') provides for injunctions against a 'service provider'. That term is given the same definition as in the *Regulations*: 'any person providing an information society service'.[74] Section 120 of the *Communications Act 2003* (UK) takes a more direct approach, defining 'intermediary service provider' as a person who, *inter alia*, 'provides an electronic communications service used for the provision of the relevant service'.[75]

(c) *European Directives*

Three Directives apply the concept of an internet intermediary. However, they give limited guidance beyond the E-Commerce Directive and *Regulations*. First, the Information Society Directive refers to intermediaries without definition.[76] Recital (33), for example, confirms that liability should not attach to a network transmission made 'by an intermediary' on behalf of third parties, provided the intermediary does not modify the information it contains. Second, the Enforcement Directive refers to 'intermediaries' in the context of injunctive relief, and again does not define the term.[77] Third, the Technical Standards Directive contains the original definition of 'information society services' discussed above.[78]

2.2 Case law

No comprehensive definition of an intermediary can be found in English or EU case law. Some descriptions are purely technical. In *QC Leisure*, for example, Kitchin J identified the 'intermediate computer servers between a web-server and the computer running a web-browser used by an end-user'.[79] In *Meltwater*, Morritt C described processes undertaken 'in a network between third

---

[73] See, eg, *Criminal Justice and Public Order Act 1994* (UK) s 166A(6); *Privacy and Electronic Communications (EC Directive) Regulations 2003* (UK) regs 2(1), 6(4); *Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007* (UK) regs 2(1), 5–7; *Tobacco Advertising and Promotion Act 2002* (UK) reg 2(4).

[74] *E-Commerce Regulations* reg 2(1); *Copyright Act* s 97A(3). See also s 191JA(3), which creates an equivalent injunction for performers' rights.

[75] *Communications Act 2003* (UK) s 120(15)(a) ('*Communications Act*').

[76] Directive 2001/29/EC [2001] OJ L 167/10 ('Information Society Directive').

[77] Directive 2004/48/EC [2004] OJ L 157/45 ('Enforcement Directive') recital (23), art 11.

[78] See above nn 62–63 and accompanying text.

[79] *Football Association Premier League Ltd v QC Leisure* [2008] FSR 789, [241] (Kitchin J) ('*QC Leisure*').

parties by an intermediary, typically an internet service provider.'[80] Other descriptions are characterised by the inconsistent use of examples and metaphor. In *Tilley*, Eady J compared internet intermediaries to the postal service,[81] which are both 'simply conduits, or facilitators, enabling messages to be carried from one person, or one computer, to another'.[82] However, in *Newzbin2*, a website blocking case considered in chapter 7, Arnold J rejected an analogy between 'an intermediary provider, such as an ISP' and the postal service, and expressed doubts about whether analogies 'are helpful in this context'.[83] Nevertheless, analogies and metaphors continue to be used. Partly this reflects the need, identified by HHJ Parkes QC in *Davison v Habeeb*, to adapt established principles to new situations involving 'internet entities' and their 'radically novel platforms'.[84]

Intermediaries are sometimes described in terms which suggest a lower degree of responsibility. For example, the Belgian Cour d'appel has explained that the public 'knows that eBay is *only an intermediary*'.[85] Similarly, where an infringing keyword advertisement is placed on a search engine, that conduct is only 'carried out by Google *as an intermediary*' on the instructions of the advertiser 'rather than by Google'.[86] Conversely, in *Newzbin* Kitchin J rejected the defendant's characterisation of its service as '*merely acting as an intermediary*' by supplying hyperlinks.[87] Common to these cases is a perception that intermediaries are not primary wrongdoers. Thus, in *L'Oréal SA v eBay International AG* Arnold J described the question as when 'an injunction [may issue] against an intermediary who is not an infringer'.[88]

Similarly, the CJEU has described 'intermediaries, such as ISPs, whose services are being used *by a third party* to infringe their rights.'[89] A more granular description was given in *Tele2*, where the Court held that ISPs could be 'intermediaries' because 'those access providers supply the user with the connection enabling [primary wrongdoing]', and lack control over the user's

---

80 *Newspaper Licensing Agency Ltd v Meltwater Holding BV* [2012] Bus LR 53, 77 (Morritt C) ('*Meltwater*'). See also Case C-5/08, *Infopaq International A/S v Danske Dagblades Forening* [2009] ECR I-6569, [54].

81 *Tilley*, [9], [24] (Eady J).

82 See *Davison v Habeeb* [2011] EWHC 3031 (QB), [38] (HHJ Parkes QC) ('*Davison*').

83 *Newzbin2*, 897 (Arnold J).

84 *Davison*, [36], [38] (HHJ Parkes QC).

85 *eBay International AG v The Polo/Lauren Company LP* [2010] ETMR 1, 9–10 (emphasis added).

86 *Interflora Inc v Marks and Spencer plc* [2009] RPC 22, 808 (Arnold J) (emphasis added) ('*Interflora*').

87 *Newzbin*1, 548 (Kitchin J) (emphasis added).

88 [2009] RPC 21, 785 (Arnold J) ('*eBay*').

89 Case C-70/10, *Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM)* [2012] ECDR 4, 64 (emphasis added).

conduct.[90] In *eBay (CJEU)*, the Advocate–General appeared to treat the concept of an 'information society service provider' as a subset of intermediaries,[91] giving 'distributors, brokers, auction houses, flea markets and real estate agents' as examples of the latter. The Court adopted a negative definition, concluding that a service provider will not act as an intermediary if

> instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, [it] plays an active role of such a kind as to give it knowledge of, or control over, those data …[92]

A similar test was accepted in *Google France* in the context of search engines.[93] In the Court's view, passivity is lost if a service provider assists users in creating or promoting particular content, since this would involve abandoning a 'neutral position' and instead playing 'an active role' in a transaction which confers actual knowledge or control. This description emphasises two important facets of intermediaries' conduit function — content neutrality and passivity — but fails to supply an all-encompassing definition.

2.3 Scholarship

Despite a large body of scholarship examining particular kinds of intermediaries and online wrongs, very few general definitions exist and no complete taxonomy has been proposed. Instead, the term is often used homogeneously to describe an undifferentiated class of actors which share little in common except that they all operate on electronic networks. Van Eecke proposes a recursive definition of 'online intermediaries' as 'intermediaries between the participants to the internet' which 'act as go-betweens between the actual creators and the receivers of information'.[94] Most other scholars define the term by example, referring to various suppliers of 'infrastructure necessary for internet activity'.[95] Lemley's definition provides a representative illustration:

---

[90] Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECR I-1227, [43]–[46] ('*Tele2*').

[91] *eBay (CJEU)* , 995, 1004 (Advocate–General Jääskinen).

[92] Ibid 1037.

[93] Joined Cases C-236/08, C-237/08 and C-238/08, *Google France Sarl v Louis Vuitton Malletier SA* [2010] RPC 19, 624 ('*Google France*').

[94] Patrick van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 *Common Market Law Review* 1455, 1455.

[95] See, eg, Matthew Collins, *The Law of Defamation and the Internet* (2nd ed, 2005) [17.03]; MacCarthy, above n 59, 1038.

> Internet intermediaries — service providers, Web hosting companies, Internet backbone providers, online marketplaces, and search engines ...[96]

Other scholars treat 'intermediaries' and 'ISPs' interchangeably. For example, Kur and Dreier refer to 'ISPs … as all those persons who provide technical support and services in and around the internet.'[97] Mann and Belzley, in their classic defence of intermediary liability, provide an incomplete definition comprising 'ISPs, payment intermediaries, and auction intermediaries.'[98] They further particularise ISPs into 'source' (host), 'destination' (retail) and 'backbone' (transmission) operators. The Organisation for Economic Co-operation and Development ('OECD') proposes a broader definition:

> 'Internet intermediaries' bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.[99]

The OECD definition delineates six sub-categories: (1) access providers; (2) hosts and registrars; (3) search engines and portals; (4) e-commerce platforms; (5) payment systems; and (6) participative networking platforms. It also distinguishes 'pure' intermediaries (which deal with third party content, goods and services) from those that publish their own content and sell their own goods.[100] These definitions are extended in section 4.

3 Intermediaries and internet architecture

The internet is a global network of computer networks which support communications services using the Internet Protocol.[101] Although this amalgam resembles an externally monolithic network, it comprises a heterogeneous set of interconnected public and private networks which are mostly decentralised and independently controlled. Interconnection is possible due to the adoption of common standards, protocols and architectures by firms investing in network infrastructure, and via interconnection and peering agreements which enable data packets to

---

96 Mark Lemley, 'Rationalizing Internet Safe Harbors' '(2007) 6 *Journal on Telecommunications & High Technology Law* 101, 101.

97 Annette Kur and Thomas Dreier, *European Intellectual Property Law: Text, Cases & Materials* (2013) 449

98 Mann and Belzley, above n 52 (ch 1), 254–5.

99 OECD, *The Economic and Social Role of Intermediaries* (2010) 9 ('*Economic and Social Role*'); OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (2011) 20 ('*Public Policy*').

100 Ibid, *Economic and Social Role*, 10.

101 Barry Leiner et al, 'Brief History of the Internet' (1995) *Federal Networking Council* <http://www.isoc.org/internet/history/brief.shtml>.

traverse between networks. Some scholars understand the internet in these relational terms, arguing that it

> is fundamentally an agreement to interconnect using an evolving set of technical protocols, which enable universal delivery of data across the network.[102]

On this view, the internet of physical devices, cables and machines is a mirage. The essence of the internet is a set of conventions and practices by which different networked systems can communicate. Some are contractually enforceable — through service level, transit, peering and multi-homing agreements — but others exist only as a delicate and inherently vulnerable co-operative amalgam,[103] which collectively we can term the internet's *architecture*.

A proper understanding of internet architecture informs our analysis of liability rules in three ways. First, architecture supplies a vocabulary with which to describe the technical functions of intermediaries and precisely define their contributions to wrongdoing. Second, architectural choices set limits on intermediaries' ability to control information, services and applications, and indirectly regulates the behaviour of tortfeasors and claimants. Third, architecture is intrinsic to the internet's growth, innovation, and low entry costs. If these properties are to be preserved, intermediary liability rules need to respect and preserve architecture rather than interfere with it. Liability rules must be 'technology-aware', which requires an appreciation of these underlying architectural values.

This section briefly introduces three principles which it is suggested are fundamental properties of internet architecture and *de facto* network rules which characterise intermediaries' services. These principles have both descriptive and normative components, the latter sometimes being invoked as a 'battle cry for Internet freedom'.[104] While they have been endorsed by scholars as principles governing the internet's core design,[105] this research does not take a position on whether the principles are *desirable* properties. Instead, it assumes that they should be maintained in some form.

---

[102] Werbach, above n 1, 1769.

[103] See Kevin Werbach, 'The Centripetal Network: How the Internet Holds itself Together, and the Forces Tearing it Apart' (2008) 42 *UC Davis Law Review* 343, 347.

[104] Jonathan Zittrain, 'The Generative Internet' (2006) 119 *Harvard Law Review* 1974, 2029.

[105] See Barbara van Shewick, *Internet Architecture and Innovation* (2010) ch 2; Edward Lee, 'Rules and Standards for Cyberspace' (2002) 77 *Notre Dame Law Review* 1275, 1322; Timothy Wu, 'Application-Centered Internet Analysis' (1999) 85 *Virginia Law Review* 1163, 1164.

3.1 The layers principle

Layering is the most basic feature of a communications network. This involves arranging its functions into a hierarchy of self-contained modules separated by logical boundaries.[106] Users and services at higher network layers can access content without understanding the technical details of its delivery because those details are abstracted and hidden in lower layers. This allows network operators to alter the functionality of particular network layers without affecting other parts of the system. Solum and Chung argue that two 'normative implications' attend this design choice: first, that internet regulation should not compromise layer separation without good justification; and second, that the layer affected by a regulation should be as close as possible to the layer on which the regulated conduct occurs.[107] In short, the layers principle posits that regulation should not interfere with the layered nature of internet architecture.[108]

Network layers are abstractions derived from the Open Systems Interconnection ('OSI') model, which describes the underlying architecture of a communications network as a stack comprising seven independent layers.[109] Each layer performs a technical function upon which layers at higher levels of abstraction rely. Under the traditional model, the lowest, foundational layer is termed the *physical layer*, which controls units of electrical hardware used in a network node. The second, *data link layer* supplies an addressing system for accessing data stored in the physical layer and correcting certain errors. Third, the *network layer* routes sequences of data — which it subdivides into units of data called 'packets' and sends along a transport path — between nodes in the network. Fourth, the *transport layer* provides end-to-end transmission of a message from source to destination according to an agreed protocol, such as TCP/IP. Fifth, the *session layer* manages connections between remote hosts. Sixth, the *presentation layer* translates data into the required format, including by decryption. Seventh, the *application layer* provides a visible service for accessing network resources, such as Hypertext Transfer Protocol (web), File Transfer Protocol (file transmission) and Simple Mail Transfer Protocol (email). These layers progressively increase in complexity, functionality and familiarity. For present purposes, they can be grouped as follows:

(a) *Physical layers*: the hardware, cables and related equipment which store and transmit data;

---

[106] House of Lords, *Personal Security*, 10.

[107] Lawrence Solum and Minn Chung, 'The Layers Principle: Internet Architecture and the Law' (2004) 79 *Notre Dame Law Review* 815, 817–18.

[108] Ibid 849–50. In their research, Solum and Chung focussed on the application of the layers principle to government regulation rather than actions between private parties.

[109] See International Organization for Standardization, 'Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model' (1994) ISO/IEC 7498-1:1994(E).

(b) *Network layers*: the routing and transport protocols which interpret and route data for higher-level applications, but which do not inspect or modify data; and

(c) *Application layers*: the protocols, content and front-end software which receive and present data to end users.

Above all the functional layers of a network sits the *content layer*, which contains the semantic payload of a communication.[110] In simpler network models, the network and application layers are sometimes abstracted into a single 'logical' or 'code' layer.[111]

One important consequence of layering is that individual layers do not need to understand the data passed to them by other layers. Instead, received data are preserved naively via a process called *encapsulation*, in which the payload from a higher layer is packaged into a unit of data compatible with the lower layers comprising a header and the original payload data. Sometimes the design of lower layers will require large higher layer payloads to be split into multiple datagrams. When data are received at their destination host, each layer verifies the datagrams then strips out the header information, passing up the payload to the next layer. This process repeats until the application receives the original message. Datagrams are treated as a pure stream of unrecognised data by lower layers. This important property allows packets to be transmitted regardless of the type of underlying computer hardware or network configuration. That suggests a second normative consequence: services at lower layers cannot, by design, understand or alter the payload of higher-layer communications data, and should not violate layer integrity by being required to do so.

The purpose of OSI architecture is to group similar network functions together while separating and hiding the details of dissimilar functions. This makes it easier to design efficient multi-purpose networks, achieve standardisation and systems interoperability, and redesign independent sub-components.[112] Layers are intrinsic to the internet's extraordinary growth and adaptability.[113] Indeed, they form its basic building blocks.

---

[110] Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Common and User Access' (2000) 52 *Federal Communications Law Journal* 561, 568.

[111] See, eg, Benkler, above n 19 (ch 1), 562.

[112] See Hubert Zimmermann, 'OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection' (1980) 28 *IEEE Transactions on Communications* 425, 429.

[113] See van Shewick, above n 105, 360–5.

3.2 The end-to-end principle

In its traditional form, the end-to-end principle requires that application-layer network functions be maintained at the edges or 'ends' of the network, rather than in interior nodes or lower layers.[114] It is a 'guiding normative principle' of network organisation,[115] which requires specialised functionality to be situated at the points where users input and receive data to and from the network. Interior points consist solely of generic or 'dumb' (and therefore interoperable) transmitters, which forward packets without asking why. Put differently, the job of the interior network is simply to carry traffic, while the ends perform computations, interpretation and other functions on the data being transmitted — they supply specific services, such as the World Wide Web, email and P2P file-sharing. As Lessig notes, this design minimalism was intentional:[116] it offers flexibility, scalability and interoperability regardless of interior network design. While these objectives are widely shared, their political impacts are more contentious: an end-to-end network makes it both more difficult and easier to conduct surveillance during transmission (difficult because intervening systems are not easily able to control or monitor traffic, easy because those systems do not guarantee any transmission security), but generally harder to block specific content from reaching the edges. The end-to-end principle also has economic consequences if traffic must be treated equally. This lowers the barriers to entry, reduces the cost of infrastructure and enables innovation by new entrants,[117] thereby reducing the power of incumbents.

End-to-end was, in various forms, a core organising principle of the early internet.[118] Although it has been weakened with the development of more complex network topologies, packet inspection and Quality of Service ('QoS'), it remains a core architectural value. The consequence of end-to-end is that most functionality visible to users is achieved at the application layer. Software innovation is decentralised because it occurs at the edges of networks, proximate to content rather than infrastructure. Network hardware innovation is, by contrast, largely centralised. Many of the economic and social benefits created by intermediaries are by-products of end-to-end architecture, since it reduces coordination costs between multiple innovators to a

---

[114] Mark Lemley and Lawrence Lessig, 'The End of End-To-End: Preserving the Architecture of the Internet in the Broadband Era' (2001) 48 *UCLA Law Review* 925, 930.

[115] Solum and Chung, above n 107, 845.

[116] Lessig, above n 26 (ch 1), 44.

[117] Oliver Williamson, *The Economic Institutions of Capitalism* (1985) 205.

[118] See Brian Carpenter, 'Architectural Principles of the Internet' (1996) (*Internet Engineering Task Force*, RFC 1958); Jerome Saltzer et al, 'End-To-End Arguments in System Design' (1984) 2 *ACM Transactions in Computer Systems* 277.

level roughly equivalent to an integrated firm.[119] Indeed, some scholars argue that without end-to-end, most network and software innovation would have been impossible.[120]

3.3 The generativity principle

The internet was designed to enable almost any type of network and device to interconnect. Using standard components, anyone could assemble a machine which was able to transfer data to and from other devices on other networks. These machines could be used by a community of decentralised innovators to produce software capable of performing almost any function on those networks. This software could then be used by anyone to send and receive content without knowing precisely how it works. Zittrain argues that the underlying architectural properties which make these behaviours possible — sometimes termed 'openness', 'autonomy' or non-discrimination[121] — reflect 'generativity': the property of a technology which can 'produce unprompted change driven by large, varied, and uncoordinated audiences.'[122] Such user-driven 'change' enables innovation and makes more useful, adaptable and powerful technology.

Generativity comprises four elements: capacity for leverage (making difficult tasks easier); adaptability (breadth of possible uses); ease of mastery (skill required to make transformative modifications); and accessibility (cost of producing derivative innovations).[123] The internet exemplifies these qualities: it reduces the costs of content creation and dissemination; it is adaptable to almost any purpose involving data; its use of encapsulation means it is easy for users to master creation in the content and application layers; and its barriers to entry are low, since anyone can interconnect with, develop and receive new edge functionality without needing permission. As a neutral, open platform, innovators can rely on common protocols to improve functionality at the application layer and know that their innovations will operate on virtually any network and device. While protocols impose their own design and performance constraints, they have proved highly resilient and central features of the internet despite rapid growth. Early attempts by network-layer intermediaries to establish 'walled gardens' of curated content and functionality failed because of their limited utility compared to the open internet. In short, the internet is the greatest example of layered network effects.

---

[119] van Schewick, above n 105, 194, 200–2.

[120] Solum and Chung, above n 107, 847.

[121] See, eg, Yochai Benkler, 'Freedom in the Commons: Towards a Political Economy of Information' (2003) 52 *Duke Law Journal* 1245, 1266, 1274.

[122] Zittrain, above n 104, 1980.

[123] Ibid 1981–2, 1988.

4 A taxonomy of internet intermediaries

This section proposes a taxonomy of internet intermediaries which is structured according to the network layer model. Its basic conceit is that an accurate understanding of liability depends on more than simply classifying an intermediary's activities (as in the E-Commerce Directive). It requires us to identify precisely a party's technical contributions to harm and situate those functions within the internet's architecture.[124] Building on the work of previous scholars,[125] this functional approach reflects the complex layering of responsibilities produced by the interposition of online services between uploaders and recipients of digital information.

This exercise serves two purposes. First, it supplies a useful structure for analysing liability in later chapters, on the assumption that different considerations arise when different functions are supplied to wrongdoers. Grouping intermediaries that facilitate by different means may misunderstand their contributions to wrongdoing and lead to the wrong liability standard being applied. By adding a second dimension of classification, we introduce a richer vocabulary for describing intermediaries and identifying their relationship to primary wrongs. Second, it introduces the background technology to this research, and illustrates the full spectrum of intermediaries — not just the classical trinity of ISPs, hosts and search engines.

The overall structure is illustrated in Figure 1:

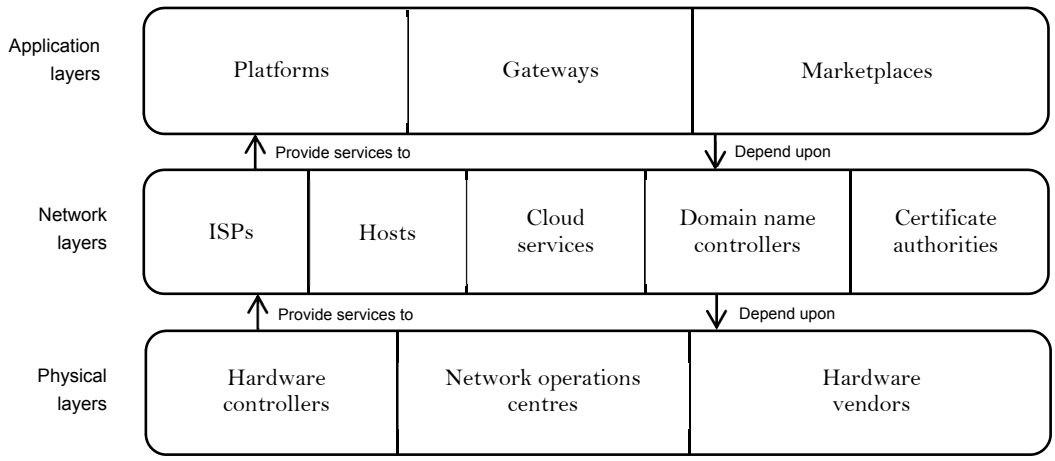

Figure 1: Internet intermediaries as layered services

[124] See, in the context of cybercrime: Cyrus Chung, 'The *Computer Fraud and Abuse Act*: How Computer Science Can Help with the Problem of Overbreadth' (2010) 24 *Harvard Journal of Law and Technology* 233, 253–6.

[125] Benkler, above n 19 (ch 1), 396, 412, 439; Solum and Chung, above n 107, 818.

Several limitations of the network layer approach should be borne in mind. First, the boundaries of services within each layer are fluid, and one intermediary may fit into multiple categories simultaneously; for example, many application-layer platforms are also gateways. Entire categories may appear or disappear as technology and consumer needs evolve; consider the supplanting of human-edited directories by indexed search engines. Being based upon abstract principles of network architecture, this taxonomy is flexible and capable of adaptation. Second, a single natural or legal person can supply services at multiple layers simultaneously; it can be commercially artificial to separate vertically integrated entities (such as Google and Facebook), which we think of as single services, into their constituent functions at each layer. Finally, certain related entities are necessarily grouped together in the same layer despite subtle (but ultimately unimportant) differences in their functions; this improves clarity but comes at the expense of taxonomic precision. The following sections provide non-exhaustive examples at each network layer.

4.1 Physical layer intermediaries

Physical layer intermediaries deal in the medium of transmission. They provide the basic connectivity necessary for communication — typically a modem, Ethernet interface, wireless access point, optic fibre or secondary storage device. Most physical layer intermediaries fall into three sub-categories. First, *hardware controllers* own or operate the physical equipment used in network backbones, servers and access points. Second, *network operations centres* own the physical environment in which hardware is stored and operated, and supply secondary resources such as electricity and connectivity. Third, *hardware vendors* build the physical equipment — cables, microprocessors, pre-assembled computers and their components — and may supply configuration and support services.

Because the physical layer is designed to be separable from higher layers, these parties rarely exercise control over content. Hardware design can place constraints on functionality — for example, by restricting the applications which can be executed on a particular device, or hard-coding technical protection measures.[126] However, in most cases physical layer equipment is simply incapable of inspecting the contents of datagrams transmitted via their network interfaces. For this reason, physical layer intermediaries are very rarely involved in disputes over liability on

[126] See, eg, the treatment of 'apps' in Apple iOS: Zittrain, above n 122 (ch 1), 182.

the (reasonable) assumption that they are simply too remote from the nexus of wrongdoing. They receive subsidiary treatment in this research.

4.2 Network layer intermediaries

Network layer intermediaries supply services to route data packets between IP addresses on the internet. Five distinct sub-classes can be distinguished, though it is not the focus of this chapter to define them in any detail.

First, an *ISP* connects its subscribers to the internet by supplying telecommunications facilities and access equipment (modems and subscriber lines). When a subscriber requests or publishes content on a third party website, the packets pass through the ISP's network and are relayed to the remote host, which transports the response back to the subscriber.[127] Although ISPs do not normally filter or examine transmitted data, they sometimes use deep packet inspection ('DPI') technology for network management and website blocking purposes. Most impose contractual terms which prohibit the use of their services to publish or access tortious content.[128] *Mobile carriers* are a distinct sub-class which supply wireless connectivity to subscribers of a mobile telephone network. Such carriers tend to impose more substantial filters on content using a border proxy, which restricts access to material, protocols and sometimes competing services.[129]

Second, *hosts* supply storage and transmission facilities that allow application-layer services to be accessed by other internet users.[130] Typically, customers lease an agreed allotment of resources measured by storage space and transmission volume, often anonymously. The relationship between hosts and their customers is primarily regulated by contract. Almost all conditions of service prohibit the publication of defamatory, copyright-infringing and other tortious content.[131]

---

[127] See Barry Greene and Philip Smith, *Cisco ISP Essentials* (1st ed, 2002) 229–34.

[128] See, eg, Tiscali UK Ltd, 'Terms and Conditions for Tiscali Broadband, Talk and TV' (2008) *Legal*, cl 6.4.1 <http://www.talktalk.co.uk/legal/tiscali-product/terms/>.

[129] See, eg, Rob Coppinger, 'iPhone 4 FaceTime is WiFi Only Says O2' (*The Inquirer*, 21 June 2010) <http://theinquirer.net/inquirer/news/1686883/facetime-wifi-o2>.

[130] Typically this means a web server and high-speed connections to a major backbone: Quinstreet Inc, 'Web Host' (2006) *Webopedia* <http://www.webopedia.com/TERM/W/Web_host.html>.

[131] 1&1 Internet Ltd, 'General Terms and Conditions of Service' (2010) *Terms & Conditions*, cl 6.2.2 <http://order.1and1.co.uk/xml/order/TcGeneral>.

Third, *cloud service providers* offer remote computational and storage services for on-demand access at network edges.[132] Services such as content distribution networks, webmail, document retrieval, customer and project management, media streaming and databases are increasingly delivered via cloud infrastructure. Like mainframe computers, cloud services offer better, cheaper functionality by exploiting economies of scale; such service providers often act as both network and application-layer intermediaries.

Fourth, *domain name controllers* administer the DNS, which is responsible for translating human-friendly domain names, such as '`ox.ac.uk`', into the IP address of the corresponding server, namely '`163.1.60.42`'.[133] Besides convenience, domain names ensure stability by allowing application-layer services to shift locations on a network without requiring addresses to be updated.[134] Of particular relevance are *TLD registry operators*, which control the registration and resolution of domain names within a particular top-level domain ('TLD') namespace, such as VeriSign Inc (`.com`, `.net`). Registries determine the eligibility of registrants for domain names,[135] operate authoritative nameservers, and maintain data about registrants in a database (known as the WHOIS database).[136] *2LD registry operators* perform a similar function in relation to country-specific namespaces, such as Nominet (`.uk`), while *domain name registrars* accept applications for the registration or renewal of particular domain names (such as `google.co.uk`) and collect personal information from registrants.

Finally, *certificate authorities* issue public keys for use in asymmetric cryptography. This involves verifying the identity of key recipients, who typically supply application-layer services.[137] Most certificates are accompanied by contractual indemnities for loss arising from malicious decryption or fraud.[138]

---

[132] Peter Mell and Tim Grance, 'The NIST Definition of Cloud Computing' (7 October 2009) <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>.

[133] See John Klensin, 'Role of the Domain Name System (DNS)' (2003) (*Internet Engineering Task Force*, RFC 3467) 2. IPv6 introduces added complications that will not be addressed here.

[134] Paul Mockapetris, 'Domain Names — Concepts and Facilities' (1987) (*Internet Engineering Task Force*, RFC 1034) 4, 18.

[135] See, eg, Nominet UK Ltd, 'Our Contracts' (2010) <http://www.nic.uk/disputes/terms/>.

[136] Leslie Daigle, 'WHOIS Protocol Specification' (2004) (*Internet Engineering Task Force*, RFC 3912).

[137] See, eg, Netcraft, 'Market Share of Certification Authorities' (2010) <https://ssl.netcraft.com/ssl-sample-report//CMatch/certs>.

[138] See, eg, Comodo CA Ltd, 'Comodo SSL Certificate Warranty' (2012) <http://www.instantssl.com/ssl-certificate-products/ssl/ssl-warranty.html>.

4.3 Application layer intermediaries

The application layer is by far the most diverse. This is where content is transacted, having been encoded, sent, transmitted, received and decoded by lower layers. Protocols such as HTTP, client software like Mozilla Firefox and web services including Google, Facebook and YouTube all operate at the application layer. These are the entities closest to end-users and with the highest degree of control over content. Although it is possible to classify application-layer intermediaries in various ways, three main sub-classes are proposed here.

(a) *Platforms*

The most common targets of intermediary liability are operators of platforms, typically websites, that display materials authored by their visitors — so-called 'user-created content'.[139] That content can take various forms, and a complete taxonomy is beyond the scope of this chapter.[140] It includes text postings, such as reviews and comments; multimedia, such as photographs and videos; metadata, such as tags, votes and location information; and ancillary functionality, such as applications, plugins and 'mashups', often using an application programming interface ('API'). Collectively, these are common features of 'web 2.0' services.[141] Such user-created content is now pervasive: some 82 per cent of the United Kingdom's top 50 websites display it in some form (see Table 2).[142]

(i) *Website operators*

Alive to the risk of tortious or inappropriate content, many website operators have deployed moderation systems for the detection and removal of undesirable materials. Techniques for moderation fall into three main categories: (1) *pre-publication* approval, which involves manual review of submissions before publication; (2) *post-publication* removal, using community moderation or content flagging; and (3) *automated* content filtering, which uses probabilistic pattern analysis to identify harmful material. Although pre-publication methods are usually more

---

[139] See OECD, *Participative Web: User-Created Content* (12 April 2007) DSTI/ICCP/IE(2006)7/FINAL <http://www.oecd.org/dataoecd/57/14/38393115.pdf> 4.

[140] For one proposal, see Stephan Hagemann and Gottfried Vossen, 'Categorizing User-Generated Content' [2009] *Proceedings of the Web Science* 155 <http://journal.webscience.org/155/>.

[141] Despite definitional disagreement, see WebMediaBrands Inc, 'What is Web 2.0' (27 February 2009) *Webopedia* <http://webopedia.com/TERM/W/Web_2_point_0.html>; Tim O'Reilly, 'Web 2.0: Compact Definition' (1 October 2005) *O'Reilly Radar* <http://radar.oreilly.com/archives/2005/10/web-20-compact-definition.html>.

[142] Popularity was measured according to the average number of daily visitors and page views, using data supplied by Alexa Internet Inc: see Alexa Internet Inc, 'Top Sites in United Kingdom' (1 February 2010) *Alexa Top Sites* <http://www.alexa.com/topsites/countries/GB>.

accurate and complete than automated or flagged moderation, they are costly and delay postings in a moderation queue for hours or days.[143] Accordingly, very few platforms use them or even require identifying information from contributors. Instead, most rely on voluntary reporting and peer review of submissions.[144]

Type of user content	Content displayed?	Identification required?	Approval required?	Community moderation?	Reporting facility?
Text	82 %	20 %	5 %	43 %	67 %
Multimedia	44 %	18 %	5 %	27 %	41 %
Metadata	52 %	4 %	0 %	8 %	4 %
Functionality	14 %	14 %	29 %	43 %	43 %

Table 2: User-created content on popular UK websites

(ii) *Social networks*

The web permits a variety of human interactions via social platforms tailored to the personal, professional, romantic or other interests of their users. Although the methods and capabilities of each social platform vary considerably, most publish user-created content to a group of users who are connected by common friendship, interests or community.[145] Three main sub-classes exist: (1) *generalist* networks, such as Facebook, Twitter and Google+, which organise text and multimedia across undifferentiated social graphs; (2) *geographic* networks, such as FourSquare, which appeal to users in particular regions or based on physical proximity; and (3) *thematic* networks, which cater to specific demographics and interests, such as LinkedIn (professionals), Academia.edu (academics) and Mendeley (authors). Social networking is popular, with 98 per cent of United Kingdom internet users holding at least one account.[146]

Social intermediaries perform several functions which equip them as influential application-layer regulators. First, they are identity providers, allowing users to authenticate around the web using a single account. Second, they collect and monetise users' activities and personal

[143] On WordPress.com, for example, some 39.3m new posts and 41.4m new comments were posted by users during February 2013. Assuming that a conservative reviewer took 3 minutes per post and 30 seconds per comment to reach a decision, it would take more than 3000 reviewers working around the clock simply to keep pace with incoming submissions.

[144] Once flagged, content tends to be removed in accordance with the website's acceptable usage policy: see, eg, YouTube LLC, 'YouTube Community Guidelines' (2010) <http://youtube.com/t/community_guidelines>.

[145] European Union Article 29 Data Protection Working Party, Published Opinion 5/2009 on Online Social Networking (12 June 2009) 4–5.

[146] comScore Inc, *Media Metrix* (October 2011).

information for targeted advertising, which makes such networks powerful gatekeepers of privacy and law enforcement.[147] Third, much of what is said and read about individuals online occurs on social networks. In the reputation economy, social networks are the dominant treasury. Finally, many social intermediaries employ staff to moderate suspicious or flagged content.[148] Such moderation is imperfect, and incidents of online harassment and bullying are well-documented.[149]

(iii) *File repositories*

File repositories (also known as 'cyber-lockers') are web-based services that allow users to upload digital files for personal storage. They provide an application-layer interface to a host under their control, to which files can be uploaded using a web browser. Examples include personal backup services such as Dropbox and one-click sharing services such as RapidShare and MegaUpload. Repositories are usually content-agnostic by design, but are the most popular sources of copyright-infringing content[150] and account for large volumes of internet traffic.[151]

(iv) *Media sharing platforms*

Platforms such as YouTube, Instagram, Flickr and Soundcloud allow their members to upload videos, images or music in permitted file formats. Other members can typically post comments — 'notorious' for their low quality[152] — and ratings. Most platforms adopt community policies which restrict the permitted types of content and normally act to remove videos or comments which breach those policies using post-moderation. YouTube also uses a statistical method known as 'Content ID' to identify copyright works contained in users' videos by matching them against a database of known works supplied by content owners. If a match is detected, copyright owners have the choice of removing the video, receiving a percentage of advertising revenues generated by its display, or monitoring traffic.[153] Although this system occasionally produces false positives[154] and fails to consider legal subtleties such as subsistence and defences, it is generally

---

147 See Michael O'Floinn and David Ormerod, 'Social Networking Sites, RIPA and Criminal Investigations' [2011] 10 *Criminal Law Review* 766, 770–2.

148 See Kashmir Hill, 'Facebook's Top Cop: Joe Sullivan' (*Forbes*, 12 March 2012).

149 See Bruce Mann, 'Social Networking Websites — A Concatenation of Impersonation, Denigration, Sexual Aggressive Solicitation, Cyber-Bullying or Happy Slapping Videos' (2008) 17 *International Journal of Law and Information Technology* 252.

150 Charles Arthur, 'Why Are Cyberlockers Suddenly Such a Problem, Lord Mandelson?' (*The Guardian*, 20 November 2009) <http://guardian.co.uk/technology/2009/nov/20/copyright-digital-economy-cyberlockers-rights>.

151 MarkMonitor, *Traffic Report: Online Piracy and Counterfeiting* (January 2011) 7.

152 Matthew Moore, 'YouTube's Worst Comments Blocked by Filter' (*The Telegraph*, 2 September 2008).

153 YouTube LLC, 'Content ID' (2011) <http://www.youtube.com/t/contentid>.

154 See, eg, Andy Baio, 'Copyright Kings are Judge, Jury and Executioner on YouTube' (29 February 2012) *Ars Technica* <http://arstechnica.com/tech-policy/news/2012/02/copyright-kings-are-judge-jury-and-executioner-on-youtube.ars>.

regarded as a gold standard in automated content moderation.[155] However, a certain level of tortious content is inevitable; one claimant alleged that 150 000 of its videos had been uploaded to YouTube without authorisation.[156] Other media platforms link to live streaming feeds for television, sporting and musical events.[157] Finally, some platforms are oriented around the concept of 'social curation', whereby users repost existing third party content. Pinterest, for example, encourages users to 'pin' items of interest to its social bulletin board, which displays images of the items sourced from third parties.[158]

(v) *Publishing services*

Publishing services provide an interface for individuals to publish documents. First, blogging services, such as Google's Blogger.com and WordPress, encompass the so-called 'blogosphere' — the tightly interlinked region of the web in which most amateur self-publishing occurs. Second, discussion fora allow users to post messages in threaded topics which are visible to other members (and often the general public). Third, document repositories such as Scribd allow their users to upload hosted text documents for public dissemination. Finally, comment and reputation tools such as Disqus provide centralised moderation and comment-hosting tools to blogs and other websites.[159]

(vi) *Location services*

Location services provide data based on the user's location. First, local directories and review websites such as Yelp, TripAdvisor and Google Maps connect reputational information to specific geographic locations (mainly restaurants, hotels and tourist attractions). Second, planning and itinerary services such as TripIt and WorldMate aggregate users' bookings and other travel content. Third, social location services such as Foursquare allow their users to 'check-in' to venues, displaying relevant information and location-aware advertising.

(vii) *Gaming platforms*

Gaming platforms mediate the delivery and consumption of electronic video games for personal entertainment. For example, virtual world operators supply the software, content and

---

155 Scott Smitelli, 'Fun with YouTube's Audio Content ID System' (2009) <http://www.csh.rit.edu/~parallax/>.

156 *Viacom International Inc v YouTube Inc*, Plaintiffs' Complaint (SDNY, 2007) [3].

157 See, eg, PlayFi Pty Ltd, 'PlayFi — Live Music' (2012) <http://playfi.com/> (music); Hulu LLC, 'Watch TV. Watch Movies. Online, Free' (2013) <http://www.hulu.com/> (television); Cricket365, 'Live Cricket Streaming' (2011) <http://www.cricket-365.tv/> (sport).

158 See Pinterest Inc, 'Pinterest' (February 2013) <http://pinterest.com/>.

159 See Discuss Inc, 'About Disqus' (March 2013) <http://disqus.com/about/>.

infrastructure that enable 'massively multiplayer online' games to function. The most prominent example is World of Warcraft, which boasts 10.2 million subscribers[160] who connect to a network of around 20 000 computers housing 1.3 petabytes of storage.[161] Smaller game developers such as Zynga create software for social networks or smartphones,[162] while gaming content distributors such as Steam sell and distribute third parties' gaming software.[163]

(b) *Gateways*

Gateways collate, index and distribute hyperlinks to third parties' internet content. Search engines, portals, directories and RSS syndication are the most common examples. While these services employ various means to locate and rank relevant material, they are united by their reliance upon automated tools and algorithms to parse, store and query large volumes of data authored by others. Content aggregation usually involves three distinct phases: (1) *crawling*: data is gathered by means of an artificial computerised agent (a 'robot') that recursively browses hyperlinks on the web and extracts page content; (2) *indexing*: extracted page content is added to a database called an index which stores instances of keywords and performs automated data analysis to determine authoritativeness and extract structured data; and (3) *retrieval*: when a query is received, relevant pages in the index are identified, ranked and presented to the user. Most aggregators include a brief extract or 'snippet' of the information alongside each result, which automatically repeats information from the source webpage using a combination of meta tags, keyword matching, structured content 'recipes' for extracting particular kinds of data (such as flight times), and statistical summation. Summaries produced by human editors are relatively infrequent.[164] Another class of gateways abbreviates URLs by allowing users to register 'shortened URLs' which instantly redirect users to the original page content.[165]

---

[160] Activision Blizzard Inc, *Q4 Earnings Call* (9 February 2012).

[161] See Ashlee Vance, 'Computing from Weather to Warcraft' (*The New York Times*, 17 November 2008) <http://nytimes.com/2008/11/18/technology/business-computing/18super.html>.

[162] Zynga Inc, Form S-1 Registration Statement, United States Securities and Exchange Commission (11 August 2011) 1–2.

[163] See Valve Corporation, 'Content Server Stats' (2 March 2012) *Steam* <http://store.steampowered.com/stats/content/>.

[164] One notable exception is the human-edited Open Directory Project: Netscape Communications Corp, 'About the Open Directory Project' (2002) *Open Directory Project* <http://www.dmoz.org/about.html>. Such aggregators are better classified as websites on the basis that their operators exercise control over the selection of content.

[165] See Thord Hedengren, 'TinyURL Blocked in Saudi Arabia' (*The Blog Herald*, 17 April 2009) <http://www.blogherald.com/2009/04/17/tinyurl-blocked-in-saudi-arabia/>.

(c) *Marketplaces*

Online marketplaces allow users to buy and sell goods and services from third parties. First, *auction websites* such as eBay facilitate transactions involving goods between vendors and purchasers. To reduce listings for infringing and counterfeit goods, eBay operates a Verified Rights Owner ('VeRO') programme consisting of around 16 000 keyword filtering rules, community moderation via flagging, restrictions on sales of 'High Risk Brands', and a notice-and-takedown system under which 90 per cent of notices led to removal within 6–12 hours, with 98 per cent removed within 24 hours.[166]

Second, *ticketing portals* such as Viagogo, Ticketmaster and LiveNation sell tickets to events and enable secondary markets for the transfer of unwanted tickets. Third, *retail emporia* such as Amazon.co.uk aggregate retailers' wares into a central marketplace of goods. Fourth, *app stores* such as iTunes and Google Play sell third parties' software and content in formats optimised for particular mobile platforms. Fifth, *classified listings* such as Craigslist and GumTree allow individuals to post notices for goods and services. Sixth, business-to-business *labour marketplaces* such as 99designs and Elance facilitate transactions between service providers and business consumers. Seventh, *social commerce websites* such as Groupon and LivingSocial offer targeted coupons and deals fulfilled by third parties.

Finally, *payment providers* supply the services and software with which value is transferred between internet users.[167] The ecosystem of electronic payment providers is vast and beyond the scope of this research:[168] PayPal processed online transactions totalling USD$118 billion in 2011,[169] while Visa exceeded $3.7 trillion on 1.9 billion issued cards.[170] It suffices to identify several distinct sub-classes: (1) *card issuers and payment networks*, such as Visa and MasterCard; (2) *market makers* for electronic currencies, such as BitCoin; (3) dedicated *online payment systems*, such as PayPal and Google Checkout, which permit horizontal consumer-to-consumer payments; (4) *transaction processing gateways*, such as WorldPay and eWay; and (5) mobile point-of-sale and 'in-app' *micropayments providers*.[171] Some also act as deposit-taking institutions which are regulated

---

[166] See *eBay*, 123–5 (Arnold J).

[167] See OECD, *Online Payment Systems for E-Commerce* (2006) 6.

[168] See further David Evans and Richard Schmalensee, *Paying with Plastic: The Digital Revolution in Buying and Borrowing* (2nd ed, 2005) 9–14.

[169] PayPal Inc, 'Financials' (January 2012) *PayPal Press Center* <https://paypal-media.com/about>.

[170] Visa Inc, *Annual Report 2011* (2011) 2.

[171] See Juniper Research, *Mobile Payment Strategies: Opportunities & Markets 2011–2015* (July 2011) 15–21, 35–44.

as banks.[172] Others are pure transaction intermediaries and regulated via a web of contracts between vendor, bank, website operator and purchaser.

Marketplace intermediaries' primary function is to provide a secure means of electronically transferring value, while minimising transaction costs and fraudulent activity.[173] Secondarily, they provide points of regulatory control. For example, users can be excluded based on the territory in which a credit card was issued. Payment networks often conduct due diligence to verify the trustworthiness of merchants for whom they process payments, voluntarily inspecting merchants' websites and removing those involved in illicit activity, particularly child pornography, controlled pharmaceuticals and unlicensed tobacco.[174]

4.4 Exclusions and limitations

Although this taxonomy comes closer to completeness than previous models, it is nevertheless incomplete and must inevitably be so. Application-layer services are rapidly evolving — their boundaries set by user behaviours rather than intrinsic properties of networks.[175] Any attempt to classify such entities further is therefore likely to be met with diminishing returns.[176] This taxonomy excludes national regulators, statutory bodies and quasi-governmental entities such as ICANN, IETF and IANA, whose conduct is regulated by contractual and public law regimes outside the scope of this research. Excluded for similar reasons are expert consultants and programmers who create the technology used by intermediaries.

5 Preliminary conclusion

This chapter has introduced the concept of an internet intermediary and argued that they are best understood as secondary facilitators who exist within a layered, modular network architecture. Although such parties may take various forms in both online and offline contexts, they are united by the attribute that they are necessary but insufficient causes of loss when wrongdoers utilise

---

[172] See Andrés González, 'PayPal and eBay: The Legal Implications of the C2C Electronic Commerce Model' (Paper presented at the 18th BILETA Conference, London, April 2003) fn 53 and accompanying text.

[173] See OECD, above n 167, 17–19, 28–30.

[174] See Mark MacCarthy, 'Deleting Commercial Pornography Sites from the Internet: The US Financial Industry's Efforts to Combat this Problem' (Evidence to House Committee on Energy and Commerce, 2006) 70–72, 1076, 1082–3.

[175] See John Helmer, 'A Taxonomy of Social Media? Forget It' (1 November 2011) *Semantico* <http://www.semantico.com/2011/11/a-taxonomy-of-social-media-forget-it/>.

[176] See Clay Shirky, 'Ontology is Overrated: Categories, Links, and Tags' (2005) *Clay Shirky's Writings about the Internet* <http://www.shirky.com/writings/ontology_overrated.html>.

their services or status to cause harm to others. Existing definitions offer only incomplete examples, but emphasise that intermediaries properly called are usually passive, neutral and technical conduits for information, services and transactions between third parties.

This chapter divided intermediaries into three distinct categories according to the technical functions they perform and the network layer in which they act. It is suggested that this taxonomy offers a more nuanced conception of their causative relationship to harm. Conventional definitions tend to ignore important technical and normative differences between distinct sub-classes of intermediaries. In legislation, policy documents and judicial decisions, they tend to be undefined or described only by reference to incomplete categories which sit uncomfortably with the modern ecosystem of online services. This risks obscuring the true reasons why some intermediaries face legal responsibility and others do not.

If hard cases are to be correctly decided, it is imperative that decision-making begin with a technically accurate, precise and architecturally-aware description of what each internet intermediary does and how that function is implicated in primary wrongdoing. This serves important descriptive, standard-setting and normative functions; in sum, it improves the accuracy and technical feasibility of liability rules and regulatory measures, and increases their compatibility with desirable properties of the internet. Later chapters will analyse liability by reference to this taxonomy; chapter 3 first introduces the concept of secondary liability.

3
The Concept of Secondary Liability

In *Revenue and Customs Commissioners v Total Network SL*, Lord Neuberger referred to the

> well-established principle that, where two or more parties join together in some way with a view to assisting or enabling one or more of them to commit a tort, all are liable for the tort as joint tortfeasors.[1]

Joint tortfeasance by common design is one example of a wider class of secondary[2] liability rules recognised in English private law. These doctrines accept that, in some cases, legal responsibility should attach to one person ('A') which is at least partly conditioned upon conduct by a third party ('B') that causes harm to a stranger ('C'). The circumstances that justify holding A liable for B's conduct are various; they depend on a combination of A's causative relationship to harm and

---

[1] [2008] 1 AC 1174, 1286 (Lord Neuberger) ('*Total*').

[2] Joint tortfeasors are, of course, individually liable for the same 'primary' tort, which has produced substantial confusion of terminology: see below § 1.3.

mental state, the nature of A's relationship with B, and extraneous considerations of fairness and policy. Liability rules with this basic structure find expression in many areas of private law, though their nature and theoretical foundations are poorly understood.

This chapter analyses doctrines of secondary liability and considers how they have been altered by immunities accorded to internet intermediaries. Its main concern is to identify how and why English private law holds a secondary actor responsible for wrongs carried out by another person. This is important because, when internet intermediaries supply services, they assist and enable a wide sphere of wrongful conduct by third party wrongdoers without necessarily engaging in that conduct themselves. This chapter begins by distinguishing primary liability, which is the ordinary type of civil responsibility recognised in law, from secondary or accessory liability, which exists under various tortious and equitable doctrines. Section 1 identifies four connecting factors commonly applied to hold secondary wrongdoers liable, but observes that they rarely apply to passive, neutral intermediaries. This reflects an underlying policy which immunises faultless but facilitative conduits. Section 2 then surveys recent limitations introduced to protect information society service providers from liability, which complement the connecting factors of tort law. Finally, section 3 concludes by evaluating the main justifications for imposing secondary liability.

1 Classifying secondary liability in private law

Secondary liability is an 'obscure and under-theorised' part of private law.[3] Much of the confusion that has bedevilled this area stems from the use of undefined, inconsistent or misleading terminology. This section therefore begins by clarifying what is meant by 'secondary liability'; namely, civil liability which is at least partly conditioned upon proof of *prima facie* wrongdoing by a third party. It then identifies three connecting factors said to justify its imposition at common law, and one in equity. These doctrines have separate institutional and remedial histories and cannot be usefully generalised. However, they indicate a consistent policy throughout English private law of holding secondary wrongdoers accountable for harms also caused by third parties when they have a normatively and causally significant relationship with primary wrongdoing, typically constituted by an assumption of responsibility for the primary wrongdoer's actions. This claimant-led policy has influenced the development of secondary liability rules against internet

[3] Peter Birks, 'Civil Wrongs: A New World' in *Butterworths Lectures 1990–1991* (1991) 55, 100.

intermediaries, but seems unlikely to offer a sufficiently granular means of regulating their obligations and business models.

1.1 Primary and secondary wrongdoing

A distinction lies between two ways in which the law classifies wrongdoing. First, a person may engage in tortious activity by his or her own acts or omissions. Such conduct is intended and directed by that person, who carries it out personally. This type of wrong is described as 'primary wrongdoing' and its originating agent is the 'primary wrongdoer' or tortfeasor. The consequences of such conduct are, in a factual sense, caused by the person who engages in it: there is strict identity between actor and acts.

Primary wrongdoing should be distinguished from secondary wrongdoing: acts or omissions by A, the secondary actor, which (1) are not independently a primary wrong, but either: (2) cause B, a primary wrongdoer, to engage in primary wrongdoing against C in a recognised way ('causative secondary wrongdoing'); or (3) establish a recognised relationship between A and B within the scope of which B engages in primary wrongdoing against C ('relational secondary wrongdoing'). Secondary wrongdoing can be preparatory — in the sense of supplying the means or preconditions for primary wrongdoing, or constituting the necessary relationship — or adoptive of prior wrongdoing. Even if causative, it must fall within a recognised category; for example, inducing or persuading B to commit a tort is secondary wrongdoing, but merely supplying assistance to B in carrying it out is not.[4]

(a) *Exclusion of independent primary duties*

In this schema, many breaches of duties involving third parties are properly classified as primary wrongs; consider, for example, the secondary actor's failure to prevent harm to C which was 'very likely' to occur in *Dorset Yacht Co Ltd v Home Office*.[5] A secondary actor may also be primarily liable in negligence for injury caused by something or someone he has a duty to control,[6] or for a related but distinct primary wrong. For example, an ISP may engage in an act restricted by copyright (such as communication or reproduction) when transmitting infringing files uploaded by its subscribers. Although these instances involve secondary conduct, they attach primary

---

4 Cf Sales, above n 51 (ch 2), 503; *French Civil Code* art 1382 (extending quasi-strict causative liability).

5 [1970] AC 1004, 1030 (Lord Reid) ('*Dorset Yacht*').

6 See, eg, *Haynes v Harwood* [1935] 1 KB 146 (driver for bolting horse); *Newton v Edgerley* [1959] 1 WLR 1031 (father for child's use of weapon).

liability to breaches of primary duties without requiring that B's conduct be actionable, and therefore do not concern us here.

(b) *Exclusion of relational secondary wrongdoing*

Relational secondary wrongdoing differs from causative secondary wrongdoing in three important ways. First, it is the status of the secondary actor or her relationship with the primary wrongdoer which is relevant, rather than the materiality of her causal contribution to primary wrongdoing. Examples of non-causative relational secondary conduct include: wrongdoing by B which occurs within the scope of her employment or agency to A;[7] unauthorised wrongdoing carried out by B but subsequently ratified by A;[8] and primary wrongdoing done on premises controlled by A.[9] Second, relational attribution is broader, encompassing all tortious conduct that occurs within the scope of the relationship. Causative doctrines only attribute conduct to A above a certain normative and factual threshold based on A's participation. Finally, the policy concerns which motivate doctrines of relational secondary wrongdoing differ substantially from those governing causative secondary wrongdoing.[10] Accordingly, relational secondary wrongdoing will not be examined in this research.

1.2 The nature of liability

Many usages of the word 'liability' can be identified. This research uses it in its most conventional sense to describe the consequence of a person being held legally responsible for an event characterised as civil wrongdoing. Although it does not seek to enter wider debates concerning the structure or purposes of tort law, it is helpful to explain what this is commonly assumed to mean. The pithy phrase 'D is liable' is shorthand for a legal formula which refers to the obligation imposed (or recognised) by a court order to supply a prescribed remedy in response to an event.[11] That event is usually, but need not always be,[12] characterised as a legal or equitable wrong. The

---

7 See *Lister v Hesley Hall Ltd* [2002] 1 AC 215. Cf *French Civil Code* art 1384(1) (extending strict liability for acts of persons for whom D is 'responsible').

8 See *Eastern Construction Co v National Trust Co* [1914] AC 197.

9 See, eg, *Famous Music Corporation v Bay State Harness Racing and Breeding Association Inc*, 554 F 2d 1213, [6] (1st Cir, 1977) (imposing liability for infringing performances on property controlled by the defendant). These cases can be viewed as breaches of a primary duty to take reasonable steps to prevent land from causing harm to others: see *Leakey v National Trust for Places of Historic Interest or National Beauty* [1980] QB 485, 517–19 (Megaw LJ).

10 See Atiyah, above n 51 (ch 2), 12–28.

11 Peter Birks, 'Rights, Wrongs, and Remedies' (2000) 20 *Oxford Journal of Legal Studies* 1, 23.

12 Stevens, above n 24 (ch 2), 58 (giving the example of a prophylactic injunction prohibiting lawful conduct).

consequence of holding D liable is that C can go to court and obtain an order for a remedy against D. The traditional function of tort law was to determine which events generate these remedial obligations and which do not.[13] It makes a defendant answerable to the claimant 'under the rules to be blamed, punished, or made to pay.'[14]

1.3 Secondary liability in tort

In *OBG Ltd v Allan*, Lord Hoffmann defined secondary liability as 'principles of liability for the act of another'.[15] Lord Nicholls described it as 'civil liability which is secondary in the sense that it is secondary, or supplemental, to that of the third party who committed [the primary tort]'.[16] A more precise definition may be that secondary liability is liability having as one of its conditions a finding of at least *prima facie* wrongdoing by a third party. For example, liability for authorising copyright infringement requires proof of actual infringement by the party so authorised. By contrast, liability for breaching a contract is primary, as it does not matter whether any third party has also breached it. Confusingly, secondary wrongdoing often leads to primary liability. Whether this is so is a question of interpreting the scope of the primary wrong. For example, s 60(2) of the *Patents Act 1977* (UK) creates a statutory tort of contributory infringement which targets secondary wrongdoing but does not require primary infringement, and is therefore an example of primary liability.[17] Similarly, unlawful means conspiracy is primary not secondary liability, since its gist is concurrence and not primary wrongdoing.[18] Secondary liability is thus closely related to the definition of a primary wrong, whose boundaries can be adjusted to encompass a wider or narrower range of conduct within it.

The doctrines of secondary liability examined in this research determine the threshold at which an intermediary will become legally responsible even though it does not independently satisfy the definition of the primary wrong. There is little to unite these disparate instances, except that they express common patterns of attribution in private law and reflect shared policies about the proper limits of personal responsibility. The term *secondary* is here used for three

---

13 Oliver Wendell Holmes, *The Common Law* (first published 1881, 1963 ed) 64.

14 Herbert Hart and Tony Honoré, *Causation in the Law* (2nd ed, 1985) 65.

15 [2008] 1 AC 1, 27 (Lord Hoffmann) ('*OBG*').

16 Ibid 59 (Lord Nicholls).

17 *Grimme Maschinenfabrik GmbH v Scott* [2011] FSR 7, 217 (Jacob and Etherton LJJ).

18 See *Total*, 1235 (Lord Hope), 1241 (Lord Scott), 1255–6 (Lord Walker), 1258–9 (Lord Mance), 1285–6 (Lord Neuberger).

reasons: first, to mirror accepted judicial practice;[19] second, to avoid 'unhelpful' and 'mistake[n]' comparisons with criminal accessory liability and the vicarious liability of employers, which carry their own conceptual burdens;[20] and third, to select a neutral label which does not assume any particular model of non-primary responsibility (such as contributory or indirect tortfeasance),[21] while recognising that we are concerned with parties whose causal contributions are individually insufficient to complete the tort. However, this label can still cause confusion. In particular, most tortious liability attaching to secondary wrongdoers is *primary* in the important sense that all wrongdoers are jointly liable for the same tort, subject to rights of contribution. Joint tortfeasors are therefore 'principals' rather than 'accessories' in the strict sense.[22]

To establish secondary liability in tort requires the claimant to show two things. First, reflecting its 'parasitic' nature, there must be some primary wrongdoing, without which it is 'self-evident' that no liability can attach to other parties.[23] For example, there can be no joint liability for trade mark infringement without a finding of primary infringement.[24] Similarly, there can be no inducement of a breach of contract without a primary breach, or interference with business by unlawful means without an independently actionable wrong: 'No secondary liability without primary liability', as Lord Hoffmann surmised in *OBG*.[25]

Second, the secondary wrongdoer's conduct must fall within a recognised connecting factor. This specifies a threshold of causative participation and knowledge which are, in combination, normatively sufficient for 'concurrent fault'.[26] This section discusses three: (1) procurement of a wrong; (2) participation in a common design to carry out a wrong; and (3) authorisation of a wrong, including by ratification. Despite some confusion,[27] these connecting factors are disjunctive 'facets' of secondary liability.[28] Together, they identify the situations when a sufficient

---

19 But see *eBay*, 762–3 (Arnold J). Cf *Total*, 1209.

20 *Credit Lyonnais*, 500 (Lord Woolf MR); *CBS*, 1059 (Lord Templeman). Labels such as 'indirect' confuse the nature of liability with the method of acting. Cf Paul Davies, 'Accessory Liability: Protecting Intellectual Property Rights' [2011] 4 *Intellectual Property Quarterly* 390.

21 Cf *Unilever plc v Gillette (UK) Ltd* [1989] RPC 584, 608–9 (Mustill LJ) (Ralph Gibson and Slade LJJ agreeing) ('*Unilever v Gillette*').

22 Pey-Woan Lee, 'Inducing Breach of Contract, Conversion and Contract as Property' (2009) 29 *Oxford Journal of Legal Studies* 511, 521.

23 *Total*, 1255 (Lord Walker).

24 *Interflora*, 815 (Arnold J).

25 *OBG*, 31 (Lord Hoffmann).

26 Glanville Williams, *Joint Torts and Contributory Negligence* (1951) 2.

27 See, eg, *CBS*, 1058 (Lord Templeman) (D liable if 'he intends *and* procures *and* shares a common design that infringement shall take place') (emphasis added); cf *MCA Records Inc v Charly Records Ltd* [2002] FSR 26, 424 (Chadwick LJ) ('*MCA Records*') (treating the test as disjunctive).

28 *Unilever v Gillette*, 595 (Mustill LJ).

nexus exists between secondary and primary wrongdoers to justify extending liability to the former. They are non-exhaustive and it would, as Bankes LJ observed in *The Koursk*, 'be unwise to attempt to define the necessary amount of connection' in the abstract.[29] For example, they are routinely supplemented by statutory secondary liability, as in the case of copyright[30] and partnerships.[31] One commonality may be that they each describe ways a secondary actor can become so involved in the primary wrong as to make those acts 'his own'.[32] In other words, these parallel criteria determine whether a secondary actor has voluntarily assumed responsibility for the primary wrongdoer's conduct.[33] The following sub-sections analyse their boundaries, arguing that all secondary liability in tort ultimately collapses into one or more heads of assumed responsibility.

(a) *Procurers*

Secondary liability for procuring arises where A intentionally causes B 'by inducement, incitement or persuasion' to engage in particular acts infringing C's rights.[34] Procurement of a tort is not a separate tort.[35] Instead, it makes the secondary wrongdoer liable as a joint tortfeasor. Correctly understood, it has two elements: physical and mental.

(i) *Physical element: 'induce, incite or persuade'*

To procure a wrong requires that A's conduct must *cause* it in the sense described previously. In *Allen v Flood*, Lord Watson expressed the principle in broad terms in the context of inducing a breach of contract:

> He who *wilfully induces* another to do an unlawful act which, *but for his persuasion, would or might never have been committed*, is rightly held to be responsible for the wrong which he procured.[36]

On this view, procurement must exert a material causal influence upon the primary wrongdoer. This is a significantly higher threshold than mere facilitation. In *Belegging-en Exploitatie Maatschappij Lavender BV v Witten Industrial Diamonds Ltd*, the Court rejected the claimant's

---

29 *The Koursk* [1924] P 140, 151 (Bankes LJ) ('*The Koursk*').

30 See below chapter 5, § 1.1 for a discussion of statutory 'authorisation' liability, which (exhaustively defining copyright) impliedly abrogates common law authorisation rights.

31 See *Partnerships Act 1890* (UK) s 10.

32 *Sabaf SpA v Meneghetti SpA* [2003] RPC 264, 284 (Peter Gibson LJ) ('*Sabaf*').

33 Cf *Caparo Industries plc v Dickman* [1990] 2 AC 605, 628–9 (Lord Roskill) (describing a duty arising from assumptions of responsibility for the performance of an activity).

34 *CBS*, 1057–8 (Lord Templeman).

35 *Amstrad*, 66 (Glidewell LJ); citing *Belegging*, 66.

36 *Allen v Flood* [1898] AC 1, 106–7 (Lord Watson) (emphasis added).

contention that 'aiding' infringement by selling a sub-component of a patented invention was procurement: 'Facilitating the doing of an act is obviously different from procuring the doing of the act.'[37] Although the dividing line can be a matter of degree, there was in that case no 'nexus' between the defendant distributor and purchasers who used its product, an industrial diamond grit, to infringe the claimant's patent. Even if the sole use of the grit was to infringe the patent, this would be insufficient: to procure, the sellers must have 'wilfully induced someone' to infringe. Similarly, in *Cadbury Ltd v Ulmer GmbH*, a distributor of generic flaked chocolate bars was not a procurer but a mere facilitator when it sold the bars to retailers who incorporated them into ice cream and thereby infringed the claimant's trade marks.[38] The inducement in these cases did not supply sufficient persuasion that without it the wrong 'would or might not have occurred'.

These cases were cited with approval by Arnold J in *eBay*, which is discussed further below. Citing *CBS*, Arnold J drew no distinction between secondary liability for trade mark infringement and other types of primary wrongdoing.[39] This suggests that, notwithstanding the distinct statutory language and policy objectives reflected in copyright, contractual and other wrongs, a unified concept of procurement applies throughout English tort law. Similarly, in *Cadbury* the Court held that the principles of joint tortfeasorship which apply to copyright 'are equally applicable' to trade marks.[40]

(ii) *Mental element: intention*

The second element focuses attention on the mental state of the procurer and how his conduct 'wilfully' sought to influence the primary wrongdoer. Ordinarily, A must intend B to engage in wrongful conduct in a particular way. This entails knowing of at least the existence of the primary right to be interfered with and the acts to be performed, while possessing any mental element necessary for primary liability.[41] This requirement distinguishes fault-based procurement liability from primary liability, which may be strict (as in the case of copyright and defamation).

(iii) *Inducing a breach of contract*

Where A intentionally procures B to break her contract with C, A may be liable under the separate tort of inducing a breach of contract. This liability derives, but is conceptually distinct, from B's

---

[37] [1979] FSR 59, 65–6 (Buckley LJ) ('*Belegging*').

[38] [1988] FSR 385, 398 (Falconer J) ('*Cadbury*').

[39] *eBay*, 766–70 (Arnold J).

[40] *Cadbury*, 404 (Falconer J).

[41] See Atiyah, above n 51 (ch 2), 290–1.

primary liability in contract.[42] As Erle J reasoned in *Lumley v Gye*, 'the procurement of the violation of a right is a cause of action in all instances where the violation is an actionable wrong'.[43] However, inducing a breach of contract has a special status because, unlike other forms of tortious procurement, it imposes secondary liability under a separate tort: the procurer is a wrongdoer in tort, while the primary wrongdoer is liable on the contract. Despite this difference, the House of Lords made clear in *OBG* that *Gye* is analogous to other forms of joint tortfeasorship.[44] Both are forms of secondary liability, in 'sharp distinction' to wrongs to which primary liability attaches. Both require proof of actionable primary wrongdoing. This difference may explain the confusion which has led some judges to treat *Gye* as a case where 'both the opera singer and the defendant were joint wrongdoers participating in an unlawful common design'.[45] Ultimately, it may be academic which description is preferred: in either case, the secondary wrongdoer is liable in tort and that liability is parasitic from the primary breach.

The most important consequence of secondary contractual liability is to extend doctrines of joint tortfeasance to non-tortious wrongs, such as breaches of contract. *OBG* did not finally resolve whether it is possible to induce a breach of 'other actionable obligations'[46] — such as procuring breach of statutory duty[47] or persuading someone to interfere in privacy — but it seems arguable that any intentional interference with legal rights might create secondary liability.[48] The question is always whether the secondary party has induced, incited or persuaded the primary breach of duty with the required knowledge and intent. As Carty concludes, procurement applies 'throughout the civil law'.[49]

(b) *Participants in a common design*

In *The Koursk*, Scrutton LJ gave the classic description of joint tortfeasors as those 'who agree on common action, in the course of, and to further which, one of them commits a tort.[50] This doctrine has its origins in *Sir John Heydon's Case*: 'all coming to do an unlawful act, and of one party, the

---

42 *OBG*, 19, 30–31 (Lord Hoffmann), 59 (Lord Nicholls), 86 (Baroness Hale), 91–2 (Lord Brown).

43 (1853) 2 E & B 216, 232 (Erle J). See also ibid 238 (Wightman J).

44 See Burton Ong, 'Two Tripartite Economic Torts' (2008) 8 *Journal of Business Law* 723, 725.

45 *CBS*, 1058 (Lord Templeman).

46 *OBG*, 62 (Lord Nicholls).

47 See, eg, *Meade v Haringey London Borough Council* (1979) 1 WLR 637, 651 (Eveleigh LJ).

48 See, eg, *Associated British Ports v Transport & General Workers' Union* [1989] 1 WLR 939, 952 (Neill LJ).

49 See Hazel Carty, 'Joint Tortfeasance and Assistance Liability' (1999) 19 *Legal Studies* 489, 507.

50 *The Koursk*, 155 (Scutton LJ).

act of one is the act of all of the same party.'[51] The basic justification for attribution is that where there is *consensus* between the parties to cause wrongdoing, all 'are active in the furtherance of the wrong'.[52] Common design is sometimes described as a broader category than procurement, since consensus is more easily demonstrated than inducement.[53] Consequently, as Mustill LJ observed in *Unilever v Gillette*, many procured wrongs will satisfy both heads.[54] However, it is also narrower, in that A must actually take part in the plan. Like procurement, common design comprises physical and mental elements.

(i) *Physical element: concerted action*

The required causal link is 'concerted action to a common end',[55] rather than independent but cumulative or coinciding acts. This entails two requirements. First, there must be *concert*: to be concerted or agreed involves an element of mutuality, rather than mere unilateral invitation, instruction or silence.[56] The agreement may be tacit or express,[57] but it must include the tortious act or omission.[58] Second, there must be *action*: 'some act in furtherance of the common design — not merely an agreement.'[59] For example, in *Douglas v Hello! Ltd [No 2]*, the publication of private photographs was sufficient 'taking part' to make their publisher jointly liable with the photographer for interfering with the claimants' privacy.[60]

(ii) *Mental element: intention*

Each secondary party must have intended that the events constituting the primary wrong occurred,[61] and must meet any state of mind required of a primary tortfeasor.[62] As Davies has argued, this sets a high bar, and courts have not abandoned 'the shackles of *CBS*' in subsequent decisions.[63] Although intent includes wilful blindness, it does not extend to reckless or negligent

---

51 (1612) 11 Co Rep 5a, 5b; 77 ER 1150, 1151.

52 Williams, above n 26, 10.

53 *eBay*, 766–7 (Arnold J).

54 *Unilever v Gillette*, 608–9 (Mustill LJ) (Ralph Gibson and Slade LJJ agreeing).

55 *The Koursk*, 156 (Scrutton LJ); *Credit Lyonnais*, 493, 499 (Lord Woolf MR).

56 *Townsend v Haworth* (1879) 48 LJ (NS) 770.

57 *Lubrizol Corp v Esso Petroleum Co Ltd [No 1]* [1992] RPC 281, 293 (HHJ Laddie QC).

58 *Unilever v Gillette*, 608 (Mustill LJ).

59 *Unilver plc v Chefaro Properties Ltd* [1994] FSR 135, 138, 141 (Glidewell LJ).

60 [2003] EMLR 28, 596–7 (Rix LJ).

61 *CBS*, 1058 (Lord Templeman).

62 *C Evans & Son Ltd v Spritebrand Ltd* [1985] 1 WLR 317, 329 (Slade LJ).

63 Davies, above n 20, 403.

failures to know.[64] By analogy, only a specific subjective intention to bring about the acts constituting the wrong will suffice.

(iii) *Mere assistance insufficient*

Simply lending assistance to a primary wrongdoer will not make the assistant secondarily liable. In *Credit Lyonnais Bank Nederland NV v Export Credits Guarantee Department*,[65] the House of Lords upheld a decision that:

> Mere assistance, even knowing assistance, does not suffice to make the 'secondary' party liable as a joint tortfeasor with the primary party. What he does must go further. He must have conspired with the primary party or procured or induced his commission of the tort … or he must have joined in the common design pursuant to which the tort was committed[66]

The Court properly rejected any general principle of secondary liability by assistance.[67] It is always insufficient that the secondary party merely assists, facilitates or witnesses the primary wrong.[68] In this respect, many common definitions of secondary liability are untenably broad.[69]

The aversion to civil assistance liability is longstanding. In one of the earliest decisions, *Townsend v Haworth*, the Court of Appeal excused a seller of chemicals used in a patented process who indemnified purchasers against infringement of the plaintiff's patent. Merely to supply, even with knowledge that the purchaser will infringe, does not make the seller 'a party with the man who so infringes'.[70] The Court of Appeal extended this principle in *Dunlop Pneumatic Tyre Co Ltd v David Moseley & Sons Ltd*, holding that even to sell an article for the *sole* purpose of enabling another to infringe a patent will not create secondary liability.[71] Later, in *Amstrad*, Lawton LJ explained the underlying policy as a concern not to enlarge the patentee's monopoly:

> mere supplying with knowledge and intent will not be enough to make the supplier himself an infringer or a joint tortfeasor with someone who is. That this should be so is surprising until one remembers … that the law

---

64 *OBG*, 29–30 (Lord Hoffmann).

65 [2000] 1 AC 486 ('*Credit Lyonnais*').

66 [1998] 1 Lloyd's Rep 19, 46 (Hobhouse LJ) (Thorpe LJ agreeing).

67 *Credit Lyonnais*, 500 (Lord Woolf MR) (Lord Slynn, Lord Steyn, Lord Clyde and Lord Millett agreeing).

68 *Haydon–Baillie v Bank Julius Baer & Co Ltd* [2007] EWHC 1609 (Ch), [262] (Morgan J). Cf *Pratt v British Medical Association* [1919] 1 KB 244, 254 (McCardie J) (describing joint liability in trespass as extending to those 'who aid or counsel, direct, or join'); citing *Petrie v Lamont* (1841) Car & M 93; 174 ER 424, 426 (Tindal CJ), which is clearly unsound today.

69 See, eg, OECD, *Public Policy Objectives*, above n 99 (ch 2), 94 (describing secondary liability as arising when a party, *inter alia*, 'facilitates' infringement).

70 (1879) 48 LJ Ch 770, 773 (James LJ), 773 (Mellish LJ).

71 [1904] 1 Ch 612, 618 (Vaughan Williams LJ), 620 (Stirling LJ), 621 (Cozens-Hardy LJ). These authorities may supply one reason for the enactment of s 60(2) of the *Patents Act 1977* (UK).

> relating both to patents and copyright is in restraint of trade. Patentees and the owners of copyright have the rights given them by statute and no others.[72]

By contrast, in *Rotocrop International Ltd v Genbourne Ltd*, the manufacturer supplied disassembled compost bins which, when assembled, would infringe the claimant's patent. In supplying the bins with assembly instructions, the vendor entered into a common design with purchasers to infringe.[73] *Belegging* also assumed that vendors could sell components 'in circumstances which in some way made them participants in' tortious uses of them.[74] In *CBS v Amstrad*, the House of Lords applied *Townsend* to reject a claim that mere sale of goods was joint tortfeasance.[75] The seller 'did not ask anyone' to infringe (which would be procurement), and there was no common design to infringe copyright, because Amstrad did not supply specific instructions or decide the purpose for which the machines should be used; purchasers did, without any agreement between them and the vendor.

(iv) *Instruments of deception*

One apparent exception to the principle that assistance is never sufficient is the doctrine of instruments of deception. In *Farina v Silverlock*,[76] for example, an injunction issued against the printer and distributor of imitation cologne labels which it sold to retailers. The Court reasoned that, by selling the labels to retailers (who may be less scrupulous), the defendant was 'thus scattering over the world the means of enabling parties to commit frauds upon the Plaintiff'.[77] This remedy recognised secondary liability for passing off where a party is 'enabling others' to engage in wrongful conduct by 'distributing the means of doing so'. The justification was said to be prophylactic: by targeting the producer of the necessary components or instruments of fraud, the Court could 'arrest the evil at its source' before any harm befell the claimant. *Silverlock* has since been described by the Court of Appeal as a case of joint tortfeasance between printer and retailer.[78] Although this appears difficult to reconcile with *Credit Lyonnais* and *Paterson*, it must be recalled that the remedy was an injunction and not damages. This is consistent with the use of the equitable protective jurisdiction to cease or prevent wrongdoing. In any case, the arrangement between printer and retailer can probably be understood as participation in a tacit common design

---

[72] [1986] FSR 159, 206 (Lawton LJ).

[73] [1982] FSR 241, 259 (Graham J).

[74] *Belegging*, 66 (Buckley LJ).

[75] *CBS*, 1055–7 (Lord Templeman). See further chapter 5, § 1.1(c)(iii).

[76] (1855) 1 K & J 509; 69 ER 560 ('*Silverlock*').

[77] Ibid 516; 563–4 (Page Wood V-C).

[78] *British Telecommunications plc v One In A Million Ltd* [1999] 1 WLR 903, 915 (Aldous LJ).

for the retailers to engage in passing off. The agreement was for one party to print and the other to sell, and thereby both to profit. It is therefore not a mere 'means' case.[79]

In other cases, enabling a passing off sounds not in tortious secondary liability but non-monetary liability in equity. Labelling cases, such as *John Walker & Sons Ltd v Henry Ost & Co Ltd*, enjoined parties who supplied inherently deceptive instruments whose natural consequence was to enable a third party to pass off his goods as another's. In *John Walker*, the first defendant made and supplied labels knowing that the second defendant would attach them to bottles that would be filled with admixtures of cane spirit and sold as Scotch whisky. Although Foster J described these as 'tortious acts', the remedy was injunction rather than damages.[80] Most recently, *British Telecommunications plc v One In A Million Ltd* enjoined a domain name registrar from using or reselling domain names which were identical to the claimants' registered trade marks.[81] The Court of Appeal upheld the conclusion that the domain names were inherently deceptive, since their entry into the WHOIS database implied a false association with the actual trade mark owner.[82] These cases establish that injunctive relief may issue to prevent equipping another with an instrument of fraud, but damages are available only where the defendant is actually a joint tortfeasor. They can accordingly be seen as instantiations of the wider principle that a party who intentionally participates in a common design to carry out tortious activity faces tortious secondary liability.

(v) *L'Oréal v eBay*

eBay supplies an example of joint tortfeasance being alleged against an application-layer internet intermediary. eBay operated a marketplace to which 7.3 million new listings for goods were published each day.[83] The claimants argued that eBay was jointly liable for trade mark infringement with registered users who sold counterfeit and parallel-imported versions of the claimants' perfume and cosmetic goods. They pointed to four features in support of a common design. First, eBay *encouraged* infringing sales by advertising listings for trade marked goods, without warning non-EEA sellers that exporting to EEA countries could infringe. Second, eBay possessed *technical and legal control* over sellers, transactions and listing content, but failed to take

---

[79] See also *Singer Manufacturing Co v Loog* (1882) 8 App Cas 15, 22 (Lord Selborne LC) (monetary liability requires more than assistance: the seller must intend deception and supply a means with no non-tortious uses, which would necessarily amount to pursuance of a tacit common design).

[80] [1970] 1 WLR 917, 933 (Foster J) ('*John Walker*'). See also *White Horse Distillers Ltd v Gregson Associates Ltd* [1984] RPC 61, 75 (Nourse J) (finding liability on the basis of a common design to pass off).

[81] [1999] 1 WLR 903 ('*One in a Million*').

[82] Ibid 924 (Aldous LJ).

[83] *eBay*, 708–9 (Arnold J). See above chapter 2, § 4.3(c).

adequate steps to prevent infringement. Its listing policies prohibited the sale of counterfeit and other infringing items, and it regularly (but imperfectly) enforced those policies against sellers.[84] Third, as a quasi-auctioneer eBay had a relationship of *proximity* to sellers, and knew infringements were ongoing. Finally, eBay made substantial *profits* from the tortious activity.

Arnold J reluctantly concluded that these features were insufficient. The starting position was that tort law imposed 'no legal duty or obligation to prevent infringement'.[85] Liability as a joint tortfeasor is the *consequence* of failing to discharge a duty (not to procure or participate in a tortious design), and not the source of such a duty. It followed that if eBay was under no duty to act, then whether or not it failed to take reasonable steps was irrelevant. The claimants' argument was therefore circular: it assumed the duty it set out to prove. All that could be said was that eBay's platform facilitated acts of infringement by sellers, but mere facilitation with knowledge and intent to profit was not enough to satisfy any known connecting factor. General encouragement to sell non-EEA goods was insufficient; if anything, eBay's takedown policies, community moderation standards and listing rules suggested the opposite conclusion. Although eBay could do more to prevent infringement, it was not legally obliged to do so.[86] However, the Court left open the possibility that eBay, like *Silverlock*, might owe non-monetary duties to prevent future infringements under article 11 of the Enforcement Directive.[87]

(vi) *Google France*

In *Google France SARL v Louis Vuitton Malletier SA*, the CJEU rejected claims of *prima facie* liability for use of the claimant's trade marks in keyword advertisements on the defendant's search engine, such advertisements not being use by the defendant.[88] However, the Court did advert to the possibility of liability attaching under 'rules of law other than' European trade mark law, potentially inviting national courts to apply domestic secondary liability rules.[89] In England, at least, this seems unlikely as a result of the combined effect of *eBay* and *CBS*.

---

84 eBay Inc, *User Agreement* (13 August 2008); ibid 718, 722 (Arnold J).

85 *eBay*, 770–1 (Arnold J).

86 Ibid 770 (Arnold J).

87 See below chapter 7, § 3.2(f).

88 *Google France*, [55]–[56], [104].

89 Ibid [57].

(c) *Authorisers*

Procurement and common design are not the only attachment points for secondary liability.[90] Atiyah and Carty each identify a third connecting factor: common law authorisation.[91] Simply granting permission to do something tortious is ordinarily insufficient for secondary liability.[92] Cases of authorisation are therefore exceptional, and generally arise in two circumstances: prospective authorisation of nuisance which is virtually certain to occur and reasonable to prevent;[93] and retrospective ratification of an agent's tort.[94] Both categories can be understood as ways in which a principal has 'made the tortious act his own' and assumed responsibility for it by licensing the tortious activity.[95] Ratification is simply the retrospective version of authorisation, occurring *after* the primary wrong.[96] Common law authorisation is of peripheral interest to a study of internet intermediaries; statutory authorisation is discussed below.[97]

1.4 Secondary liability in equity

In parallel to the common law connecting factors, personal liability attaches in equity to one who dishonestly procures or assists in a breach of fiduciary duty.[98] Like its common law cousins, it has two elements. First, the secondary party must have materially assisted the primary breach.[99] This liability is properly described as causative, since, 'if there is no causative effect and therefore no assistance given by the [defendant] ... the requirements of conscience [do not] require any remedy at all.'[100] It is also derivative, since it cannot arise without a primary breach of duty. Second, the secondary party must have acted with 'consciousness of those elements of the transaction which make participation transgress ordinary standards of honest behaviour'.[101] This liability is therefore fault-based[102] and, although parasitic, exists independently of any remedies

---

90 *Unilever*, 602 (Mustill LJ).

91 Carty, above n 49, 495; Atiyah, above n 51 (ch 2), 292–4.

92 *Robinson v Vaughton & Southwick* (1838) 8 C & P 252, 255 (Alderson B).

93 *Harris v James* (1876) 45 LJ QB 545, 546 (Blackburn J).

94 *The Koursk*, 155 (Scrutton LJ).

95 Susan Bright, 'Liability for the Bad Behaviour of Others' (2001) 21 *Oxford Journal of Legal Studies* 311, 320–1.

96 *Wilson v Tumman* (1843) 6 M & G 236, 242 (Tindal CJ).

97 See below chapter 5, §1.1.

98 *Royal Brunei Airlines Sdn Bhd v Tan* [1995] 2 AC 378, 392 (Lord Nicholls) ('*Royal Brunei*').

99 It remains unclear whether passive involvement is sufficient: see *Satnam Investments Ltd v Dunlop Heywood & Co Ltd* [1999] FSR 722, 743 (Nourse LJ).

100 *Brown v Bennett* [1999] 1 BCLC 649, 659 (Morritt LJ).

101 *Barlow Clowes International Ltd (in liq) v Eurotrust International Ltd* [2006] 1 WLR 1476, 1481 (Lord Hoffmann).

102 *Grupo Torras SA v Al-Sabah [No 5]* [2001] Lloyd's Rep Bank 36, 62.

available against the defaulting fiduciary.[103] For example, the fiduciary may be liable to account for profits made from their wrongdoing, while the assistant may make no profit but be liable to pay equitable compensation for any shortfall.

Dishonest assistance is sometimes described as a 'general principle of "accessory liability"' in equity.[104] On this view, it would grant relief against those who dishonestly assist breaches of confidence and other equitable wrongdoing.[105] Some authorities suggest an even more general principle of inducing breach of equitable duty[106] or 'equitable fraud in a third party knowingly to assist in a breach of trust, confidence, or contract by another'.[107] Stevens argues that dishonest assistance 'is a tort in all but name.'[108] However, it remains a separate and parallel doctrine to joint tortfeasance. It is justified by the special status of a fiduciary relationship, which is characterised by the voluntary assumption of responsibility by the fiduciary[109] and vulnerability of the principal.[110] Without an equivalent relationship at common law, the prophylaxis of dishonest assistance is limited to equitable wrongs. Assistance, however dishonest, is insufficient in tort.[111]

1.5 Preliminary conclusion

Secondary liability is liability that requires proof of at least *prima facie* wrongdoing by a third party. Doctrines of secondary liability set outer limits on the outer margins of tortious responsibility for primary wrongs perpetrated by others. Their operation begins at the penumbra of primary wrongs and ends at the limits of the four connecting factors identified in this section: procurement, common design, common law authorisation, and dishonest assistance in equity. They operate as limited exceptions to the general principle that a claimant's rights extend only to those who have done him wrong. Although they developed in different institutional and doctrinal settings, they are united by the common principle that a secondary wrongdoer may be made to

---

[103] *Michael Wilson & Partners Ltd v Nicholls* (2011) 244 CLR 427, 457–8 (Gummow ACJ, Hayne, Crennan and Bell JJ).

[104] *Farah Constructions Pty Ltd v Say-Dee Pty Ltd* (2007) 230 CLR 89, 160–1.

[105] Charles Mitchell, 'Assistance' in Peter Birks and Arianna Pretto (eds), *Breach of Trust* (2002) 139, 152 (citation omitted).

[106] See *Prudential Assurance Co Ltd v Lorenz* (1971) 11 KIR 78.

[107] *Thomas v Pearce* [2000] FSR 718,720 (Buxton LJ); citing Roger Toulson and Charles Phipps, *Confidentiality* (1st ed, 1996) 92.

[108] Stevens, above n 24 (ch 2), 283.

[109] See James Edelman, 'When Do Fiduciary Duties Arise?' (2010) 126 *Law Quarterly Review* 302.

[110] See, eg, *Bristol and West Building Society v Mothew* [1998] Ch 1, 18.

[111] However, dishonest assistance may eventually approach a level which permits an inference of procurement.

answer for the wrongs of others where he has by his own conduct assumed responsibility so as to 'make them his own'.

As Aldous LJ observed in *One in a Million*, secondary liability is 'evolving to meet changes in methods of trade and communication as it had in the past.'[112] However, despite its inherent flexibility, cases like *eBay* demonstrate the futility of using secondary liability rules to regulate internet intermediaries. The now-axiomatic principle that mere assistance is insufficient absent a fiduciary relationship presents an 'insurmountable' standard of fault for claimants to satisfy.[113] Without obvious inducement of wrongdoing, conduct by neutral network- and application-layer services will rarely be sufficient. In most cases, those services expressly exclude responsibility and act as mere facilitators. The default policy choice embedded in these doctrines therefore exonerates passive conduits who play no intentional role in wrongdoing, despite knowingly facilitating it or making it a necessary part of their business models. In *eBay*, Arnold J expressed 'considerable sympathy' for the view that intermediaries should be required to do more to internalise the cost of new forms of infringement made possible by their platforms, but nevertheless concluded that joint tortfeasance offered no basis for liability.[114] It must therefore be seriously questioned whether these doctrines permit adequate evolution in '[t]he attitude of the court to the liability of one person in respect of the activities of another'.[115]

Three further shortcomings can be identified. First, secondary liability lacks granularity. Its binary nature forces courts to choose between complete immunity and joint liability, while offering no express mechanism to moderate secondary wrongdoers or allocate proportionate responsibility once admitted within the gates of liability. Doctrines of contribution could alleviate this concern, but this often means shifting the risk of non-recovery to the less blameworthy party. Second, joint liability is not concerned to ensure that policy objectives underlying primary wrongs are maximised; those wrongs may themselves furnish better tools for doing so. Third, in many cases the connecting factors themselves are vague, overlapping and empty of content. Because they are parasitic on primary rights, arguments that an intermediary is liable as a secondary tortfeasor are often circular, since they assume the existence of a duty to police or prevent primary wrongdoing. For this reason, they are often redundant, since extended primary duties have

---

[112] *One in a Million*, 486 (Aldous LJ).

[113] See Lievens, above n 58 (ch 2), 518–19.

[114] *eBay*, 769 (Arnold J). Implicit in this view is the assumption that creators of application-layer services which disrupt established commercial practices owe a duty to return the marketplace to the *status quo*. However, Arnold J did not consider that another reason why infringements occur in such quantities on eBay and other online marketplaces may be related to market segregation and price discrimination practices voluntarily adopted by claimants.

[115] *Amstrad*, 198 (Whitford J).

developed which mirror the functions of secondary liability doctrines. These arguments are developed in the context of specific wrongs in chapters 4 and 5.

2 European limits on secondary liability

Set against general law doctrines of secondary liability, European law imposes various limits on the primary and secondary liability which may be imposed upon intermediaries. These limits fall into four categories: first, safe harbours which insulate passive, neutral and technical service providers from all forms of monetary liability for transmitting, caching and storing third parties' information until put on notice of wrongdoing; second, protection from general duties to monitor third parties' information; third, limits necessary to protect fundamental rights; and fourth, general limits on injunctive relief. In practice, many of the conditions which must be satisfied to activate these protections are the inverse of conditions required to impose *prima facie* joint liability, so the regime adds little to existing limits inherent in secondary liability rules; its main contributions relate to primary liability.

2.1 Safe harbours

The E-Commerce Directive was intended to serve two important purposes. First, it aimed to secure the 'free flow of information' and promote the continued development of electronic networks.[116] As Advocate–General Maduro explained in *Google France*, the Directive sought 'to create a free and open public domain on the internet'. Safe harbours were seen as intrinsic to these objectives because of the need for intermediaries to 'remain neutral as regards the information they carry or host'.[117] Second, the Directive was intended to harmonise national approaches to intermediary content liability, minimising legal uncertainty for cross-border service providers, reducing the cost of internet services and lowering barriers to new entrants.[118]

Neither the safe harbours nor substantive rules of European Union law purport to harmonise secondary liability.[119] Instead, they effect partial harmonisation by stipulating mandatory conditions for the absence of liability. However, the conditions attaching to immunity

---

[116] European Commission, *First Report on the Directive on Electronic Commerce* (2003) 12–13.

[117] *Google France*, 602–3 (Advocate–General).

[118] E-Commerce Directive recitals (5), (40); *Tilley*, 1252 (Eady J).

[119] *eBay*, 762 (Arnold J). *eBay (CJEU)*, 995 (Advocate–General).

under articles 12, 13 and 14 mean that they are inherently unlikely to apply in circumstances where an English intermediary would otherwise face secondary liability. For this reason, they are not properly termed 'exceptions to liability' but rather 'restatements or clarifications of existing law'.[120] Further, as noted in chapter 1, the safe harbours do not protect intermediaries from non-monetary secondary liability.[121] This section briefly introduces the safe harbours, which are reconsidered in specific contexts in chapters 4–7.

(a) *Mere conduits*

Regulation 17(1) of the *E-Commerce Regulations* transposes article 12 of the Directive. It protects conduits that satisfy four negative requirements: first, *non-authorship* — the intermediary must be 'in no way involved' in authoring the transmitted information; second, *non-initiation* of transmission; third, *non-interference* in transmission; and fourth, *impermanence* of transmission data, which must not be stored beyond a period reasonably necessary for carrying out the transmission (in practice, measured in milliseconds). These requirements largely restrict the safe harbour to passive and temporary transmissions by network layer intermediaries, such as relaying IP datagrams to a remote system.[122] However, it will apply despite automated technical steps being carried out that do not affect data integrity, such as encryption and error checking.[123] In essence, this safe harbour confirms that mere assistance by passively transmitting will not be sufficient for liability.

(b) *Caching*

Regulation 18, which transposes article 13 of the Directive, protects service providers from liability for caching, which involves creating local copies of third parties' data to reduce bandwidth utilisation and access times.[124] To qualify for protection, caching must be 'automatic, intermediate and temporary', and for the sole purpose of making onward transmission more efficient.[125] Cached material must not be modified by the caching agent or cached in violation of access or storage

---

[120] *eBay (CJEU)*, 1008 (Advocate–General).

[121] See above chapter 1, § 3.3; E-Commerce Directive recitals (40), (41), (47), (48), (52).

[122] See Collins, above n 95 (ch 2), [17.09]; *Gatley on Libel and Slander* [6.28].

[123] E-Commerce Directive recital (43).

[124] See Blue Coat, 'A Technical Review of Caching Technologies' (17 December 2007) *Bitpipe.com* <http://www.bitpipe.com/detail/RES/1246303638_415.html>.

[125] *E-Commerce Regulations* r 18(a). See *Tilley*, 1256–7 (Eady J).

conditions contained in industry standard metadata.[126] Unlike conduits, caches are subject to the further requirement that they act expeditiously to remove cached information upon obtaining actual knowledge that the original copy has been removed or its removal ordered by a competent authority.[127] In assessing whether a service provider has the necessary knowledge, the Court must have regard to whether a valid notice was received, and whether the notice included certain mandatory information.[128]

The caching safe harbour has been described as a 'half way house between mere transmission and "hosting"'.[129] Collins observes that this creates 'a degree of tension', in the sense that caching must be automatic but still comply with access conditions and removal requests, which can require intervention.[130] However, because most caching proxies are designed to read metadata and remove expired pages automatically, it is suggested that the tension is not all that significant in practice. Like the mere conduit safe harbour, it excludes monetary liability for passive and technical assistance.

(c) *Storage*

Regulation 19, which transposes article 14 of the Directive, protects service providers when they store third parties' tortious material while having neither actual knowledge of the 'unlawful activity or information' nor an awareness of facts or circumstances from which that 'would have been apparent'.[131] It provides 'a powerful and clear defence' to intermediaries,[132] subject to four qualifications. First, it applies only to storage activities as such. Activities which go beyond storage — such as advertising and content creation — are unprotected, subject to other defences or safe harbours. Only limited forms of network-layer assistance are immunised, while more interventionist application-layer activities are not.

Second, as the CJEU clarified in *Google France*, storage must be 'of a mere technical, automatic and passive nature', in the sense that the intermediary is 'neutral' as regards stored data and does not play an 'active role' which confers knowledge or control of those data.[133] Although

---

[126] *E-Commerce Regulations* r 18(b)(i), (ii), (iii).

[127] *E-Commerce Regulations* r 18(b)(v).

[128] *E-Commerce Regulations* reg 22.

[129] *Gatley on Libel and Slander*, 169, [6.29]; *Tilley*, [51] (Eady J).

[130] Collins, above n 95 (ch 2), [17.12].

[131] *E-Commerce Regulations* reg 19(a)(i).

[132] *Tamiz*, [57]; *Davison*, [64].

[133] *Google France*, [113]–[114].

the neutrality requirement probably stems from a mistaken reading of recital (42) (which applies only to caching and transmission), it was upheld in *eBay (CJEU)*: if an intermediary optimises or promotes users' content, it may not be neutral.[134] Conversely, neutrality will not be defeated by a technical mechanism which automatically guides recipients of the service in creating stored data. Third, like mere conduit protection, regulation 19 requires the stored information to have been provided by a third party over whom the service provider lacked authority or control. This seems to exclude most situations of primary or relational secondary wrongdoing.

Finally, upon obtaining the necessary knowledge or awareness, the service provider loses protection unless it acts expeditiously to 'remove or disable access' to the unlawful information.[135] Although disputed,[136] the better view is that article 14, read in conjunction with article 15(1), refers to actual rather than constructive knowledge, and to past or ongoing rather than future tortious activity.[137] It is sufficient to have actual knowledge of facts or circumstances from which a 'diligent economic operator should have identified the illegality in question',[138] which suggests a hybrid standard of knowledge that assesses what the defendant actually knew according to the standards of a reasonable service provider in the defendant's position. In this respect, it invites comparison to concepts of 'dishonesty' in equity. Once knowledge has been acquired, the safe harbour will not apply to repeated infringements by the same user of the same right.[139] Specific notice-and-takedown procedures are delegated to member states,[140] and remain far from uniform.[141]

2.2 Monitoring

Article 15(1) of the Directive prevents member states from imposing general obligations upon service providers to monitor (*surveiller*) information or to investigate tortious activity. In *BT*, a case discussed in chapter 5, Parker J gave the former phrase its ordinary and natural meaning: 'to inspect or examine some phenomenon.'[142] This usually involves ascertaining whether transmitted

---

134 Cf *eBay (CJEU)*, [140]–[146] (Advocate–General).

135 *E-Commerce Regulations* r 19(a)(ii). See below chapter 4, § 3.2.

136 Cf Søren Sandfeld Jakobsen, 'Mobile Commerce and ISP Liability in the EU' (2010) 19 *International Journal of Law and Information Technology* 29, 46.

137 *eBay (CJEU)*, [162]–[163] (Advocate–General).

138 Ibid [120], [124].

139 Ibid [168] (Advocate–General).

140 E-Commerce Directive recital (46), art 14(3).

141 European Commission, *Online Services, Including E-Commerce, in the Single Market* (2012) 39–46.

142 *BT*, [114] (Parker J).

or stored information is lawful or otherwise permissible. Monitoring is 'general' when it is a systematic arrangement requiring random or universal inspection, rather than relating to individual notified instances — for example, judicial or administrative orders requiring monitoring of 'a specific site during a given period of time' to prevent 'specific' tortious activity.[143] Thus, an order requiring an intermediary to identify or terminate access to a specified wrongdoer request would not involve monitoring or investigating information because it related to a particular instance. The *Regulations* do not directly transpose this principle, which instead functions as an upper boundary on liability arising from breach of monitoring duties.

2.3 Fundamental rights

In the context of intellectual property, the CJEU has made clear that both monetary and non-monetary forms of secondary liability must strike a 'fair balance' between the rights of claimants, intermediaries, and internet users. Further, article 52(1) of the *Charter* requires any limitations upon fundamental rights to be necessary, proportionate and pursue a recognised objective. Although these principles do not directly limit common law doctrines of secondary liability, they serve as reliable guides in cases involving *Charter* rights. In *Productores de Música de España (Promusicae) v Telefónica de España SAU*, the Court approached this balancing exercise by enumerating and weighing the relevant primary rights and any fundamental rights of individuals that would be engaged by liability.[144] For present purposes, relevant primary rights include the right to property, which includes intangible property such as copyright,[145] and the right to protection of reputation and private life.[146]

Three rights of intermediaries are commonly engaged. First is the freedom to conduct a business.[147] In *Scarlet*, the CJEU held that a national injunction which required an ISP to monitor all electronic communications in perpetuity would seriously infringe this freedom: compliance would be costly, complicated and intrude upon legitimate transmissions.[148] This suggests a general limitation based on the degree of adverse economic impact upon intermediaries' business

---

[143] European Commission, Explanatory Memorandum, E-Commerce Directive IP/00/442 (4 May 2000); E-Commerce Directive recital (47); *Anheuser-Busch Inc v Portugal* (2007) 45 EHRR 36, [69]–[72]; *BT*, [111], [116], [118] (Parker J).

[144] Case C-275/06 [2008] ECR I-271, [68] ('*Promusicae*').

[145] *Charter* art 17(2); *Convention* art 1, protocol 1.

[146] *Charter* arts 7, 8(1); *Convention* arts 8, 10(2).

[147] *Charter* art 16.

[148] *Scarlet*, [46]–[49].

operations. Second, intermediaries have the freedom to supply cross-border services.[149] This is reinforced in intellectual property actions by the requirements of articles 3(2) and 11 of the Enforcement Directive that injunctions must not create 'barriers to legitimate trade'. For example, remedies could not prevent resale of genuine, EEA-authorised goods in an online EU marketplace.[150] Third is freedom of expression, which includes commercial expressions.[151] Similarly, recital (2) of the Enforcement Directive confirms that enforcement measures 'should not hamper freedom of expression … including on the internet.'

Finally, remedies against intermediaries must not unjustifiably infringe the rights of their customers. First, internet users have the rights to respect for private and family life — and, in particular, for communications — and to protection of their personal data.[152] However, this is subject to protection of the rights of others. For example, article 15 of the PEC Directive[153] permits derogations for that purpose. In *Promusicae*, the Court construed article 15 broadly, and suggested that it may include claims by authors to enforce their right to property in civil proceedings.[154] Conversely, systematic DPI analysis of customers' traffic and IP addresses may infringe this right, presumably on the basis that the level of intrusion is disproportionate.[155] Second, article 36 of the *Charter* recognises access to 'services of general economic interest'; although this falls short of a substantive right[156] and its scope has not yet been clarified, it may encompass universal service obligations to supply access to the internet.[157]

Third, users have the right to freedom of expression, which includes the freedoms to receive and impart information and ideas.[158] As the Court held in *Scarlet*, this right could be infringed by a system of blocking which could not distinguish between tortious and non-tortious material.[159] Of course, like property and privacy, this right is not absolute; it is constrained by the 'rights of

---

[149] *TFEU* art 56. See also E-Commerce Directive art 3(2) (prohibiting certain restrictions on freedom to provide information society services from another member state), annex 1 (exempting copyright and related rights).

[150] *eBay (CJEU)*, [140]–[141].

[151] *Charter* art 11; *Convention* art 10(1). See *eBay (CJEU)*, [49]–[50] (product listings in a marketplace).

[152] *Charter* arts 7, 8(1); *Convention* art 8.

[153] Directive 2002/58/EC [2002] OJ L 201/37 ('PEC Directive'), as amended by Directive 2006/24/EC [2006] OJ L 105/54 ('Data Retention Directive').

[154] *Promusicae*, [52].

[155] *Scarlet*, [50]–[51].

[156] Cf La Rue, above n 107 (ch 1); Décision n° 2009-580 (Conseil Constitutionnel, 10 June 2009) [16]; BBC, 'Finland Makes Broadband a "Legal Right"' (1 July 2010) <http://bbc.co.uk/news/10461048>.

[157] See Jacques Vandamme (ed), *Services of General Interest in Europe* (2004) 122–3.

[158] *Charter* art 11(1); *Convention* art 10(1).

[159] Case C-70/10, *Scarlet Extended SA v Société des Auteurs, Compositeurs et Éditeurs SCRL* [2011] ECR-I 0000, [52] ('*Scarlet*').

others'.[160] For example, a 'narrow and targeted' order blocking access to defamatory or infringing materials may be necessary and proportionate.[161] Conversely, restrictions on access might constitute disproportionate interferences if they impaired 'the very substance of the rights guaranteed'.[162] These rights, and the correct approach to proportionality, will be discussed further in chapters 4–7.

2.4 Injunctions

Since the decisions of the CJEU in *eBay (CJEU)* and *Scarlet*, it is clear that European law imposes freestanding upper limits on injunctive relief available in intellectual property cases. Although the 'conditions and procedures relating to such injunctions' are left to member states,[163] national measures, procedures and remedies are limited in two ways. First, they must be 'fair', 'equitable' and not 'unnecessarily complicated or costly'.[164] Second, they must be 'effective, proportionate and dissuasive', without creating barriers to legitimate trade.[165] This is commonly understood as a general requirement of proportionality.[166] In *Scarlet*, this required the injunction to reflect 'a fair balance' between the claimant's right to property and the ISP's freedom to conduct a business.[167] Conditions on injunctions are discussed further in chapters 6 and 7.

3 Explaining secondary liability

Secondary liability rules sit uneasily within the normative and conceptual structure of English private law. They constitute exceptions to the principle that a person should normally be responsible only for her own voluntary behaviour. For example, in *Weld-Blundell v Stephens*, Lord Sumner commented:

> In general (apart from special contracts and relations and the maxim *respondeat superior*), even though A is at fault, he is not responsible for injury to C which B, a stranger to him, deliberately chooses to do.[168]

---

160 See *Charter* art 52(1); *Convention* art 10(2).

161 *Newzbin2*, [200] (Arnold J).

162 Case C-112/00, *Schmidberger v Republik Österreich* [2003] ECR I-0000, [80].

163 Enforcement Directive recital (23); Information Society Directive recital (59).

164 Enforcement Directive art 3(2). See *eBay (CJEU)*, [139], [141]–[144], [155].

165 Enforcement Directive arts 3(1), 3(2). See *Scarlet*, [36].

166 See, eg, *Golden Eye*, [116] (Arnold J); *Dramatico [No 2]*, [10] (Arnold J).

167 *Scarlet*, [49].

168 [1920] AC 956, 986 (Lord Sumner).

The limits examined above further confine the exceptions recognised by tort law. Underlying them is the intuitive claim of moral philosophers that a person is responsible for 'all and only his intentional actions'.[169] Actions (or, it might be added, inactions) by others are not ordinarily our responsibility; they are theirs to bear alone. Although some scholars have attempted to derive 'general principles of accessory liability' from these disparate instances,[170] courts have consistently rejected those attempts, and the area is instead characterised by 'systematic failure' to explain the basis of principles which are frequently 'unstructured, unprincipled and incoherent'.[171] Partly this reflects terminological confusion, and partly the diverse policies, fact-specific circumstances and remedial values that these principles uphold in different areas of law.

While the purpose of this research is not to defend the coherence of secondary liability or articulate its rationale, it is helpful to conclude by briefly examining two sets of justifications for imposing secondary liability upon intermediaries. The first understands these rules as methods of attributing blame to secondary actors who have *assumed responsibility* for primary wrongdoers or their actions. This account is entirely consistent with conventional principles of tortious responsibility. Second, at the level of consequentialist analysis, secondary liability rules are supposed to reduce enforcement costs and encourage optimal policing by secondary actors who are likely to be least-cost avoiders.

3.1 Normative justifications

Modern accounts of tort law describe a system of relational directives which impose responsibility for acts or omissions which interfere with the rights of others in prescribed ways.[172] Primary tortious liability reflects the *defendant's* violation of an obligation not to do wrong to the claimant; remedies are therefore normally only available against 'the rights violator', for wrongdoing 'at the hands of the defendant'.[173] Thus, as Goldberg and Zipursky argue, the power to exact a remedy is available against wrongdoers 'only if *they* have violated the victim's right'.[174] The availability of remedies against non-violators poses a challenge to an account premised on rights or civil recourse. Either victims of wrongdoing have an entitlement to relief against parties who have not themselves infringed their rights, or — perhaps more plausibly — tort law must embed additional

---

169 John Mackie, *Ethics: Inventing Right and Wrong* (1977) 208.

170 See, eg, Sales, above n 4, 502; Davies, above n 20.

171 Claire McIvor, *Third Party Liability in Tort* (2006) 1.

172 See, eg, John Goldberg and Benjamin Zipursky, 'Rights and Responsibility in the Law of Torts' in Donal Nolan and Andrew Robertson (eds), *Rights and Private Law* (2012) 251, 263.

173 Ibid 268.

174 Ibid 273 (emphasis added).

rights against secondary wrongdoers. Theoretical responses to this challenge fall under four main headings. These are not mutually exclusive categories; instead, they supply related but distinct explanations for extending responsibility.

(a) *Holding causes of harm accountable*

The first category points to the secondary wrongdoer's causally significant conduct — encouragement, assistance, inducement, and so on — as justifying personal responsibility (with corresponding extensions of victims' recourse) for the consequences. As Hart and Honoré argue, to instigate or supply the means or other assistance 'may in a broad sense be said to give rise to a causal relationship'.[175] Gardner identifies causality — that is, actually 'making a difference' to the primary wrong — as the defining attribute of secondary responsibility and the essential difference between primary and secondary wrongdoers: while both contribute to wrongdoing, only secondary wrongdoers make their contribution *through* primary wrongdoers.[176] This explains why secondary wrongdoing must actually be a *sine qua non* of primary wrongdoing.[177] Superfluous and ineffectual contributions are ignored. Similarly, contributions which would have been effective, but which do not ultimately eventuate in wrongdoing, are forgotten. Causation thus offers a normative justification for imposing tortious liability upon a secondary party: if we are morally responsible for our voluntary conduct, then we ought also to be held responsible for wrongful consequences that conduct causes.[178]

Causation supplies a rich vocabulary with which to analyse the 'substitutional visiting of sins' upon those who set others in motion.[179] However, the romanticisation of wrongs as billiard balls, which follow deterministic paths of cause and effect, hides a great deal of complexity. First, causation does not always appear necessary for civil secondary liability: ratification may occur after the tortious conduct and have no effect on its occurrence; relational doctrines may impose liability regardless of the principal's causative role. Stevens goes further and argues that only procuring requires a causal link[180] — though this ignores the causal element of authorisation and common design, which may also 'bring about' harm by clothing the primary wrongdoer in

---

[175] Hart and Honoré, above n 14, 388. See also Wigmore, 'A General Analysis of Tort-Relations' (1895) 8 *Harvard Law Review* 377, 386–7.

[176] See, eg, John Gardner, *Offences and Defences* (2006) 58, 71–4.

[177] See, eg, K J M Smith, *A Modern Treatise on the Law of Criminal Complicity* (1991) 6–7, 66, 82.

[178] Jerome Hall, 'Interrelations of Criminal Law and Torts: I' (1943) 43 *Columbia Law Review* 753, 775–6.

[179] See Philip James and David Brown, *General Principles of the Law of Torts* (4th ed, 1978) 356.

[180] Stevens, above n 24 (ch 2), 254.

authority or giving a plan the legitimacy of consensus. Second, causation is an incomplete explanation, since merely causing or contributing to primary harm is never sufficient for secondary liability. The danger of extending liability too far for mere causal interference in primary rights can be seen by the 'wretched development'[181] of interference with performance.[182] Instead, as Hall observes, further principles of culpability — 'a body of value-judgments formulated in terms of personal responsibility' — are needed to determine *which* consequences individuals should be accountable for causing. These principles (reflected in secondary liability rules) ultimately rest on normative claims about justice, personal responsibility and the allocation of losses which cannot be defended using causation alone.

(b) *Fictional attribution to secondary wrongdoers*

Some scholars argue that secondary liability rules attribute actions to the secondary wrongdoer, as expressed by the maxim *qui facit per alium facit per se*.[183] Under this fiction, secondary wrongdoers are held responsible for conduct they are deemed to carry out which infringes the claimant's rights.[184] Older cases tend to support this view, which is traceable to *Sir John Heydon's Case*: the *acts* of any participant in the plan were imputed to all other participants, so that 'the act of either was the act of both'.[185] Some modern theorists have embraced this fiction to explain joint tortfeasorship: Atiyah argues that the secondary wrongdoer has 'effectively committed the tort himself, and the liability is not truly vicarious'; while Stevens argues that all secondary liability involves attributing actions, leading to liability 'for the same tort'.[186]

This amounts to an agency-based explanation: it treats primary wrongdoers as implied agents of secondary wrongdoers, where the 'physical acts and state of mind of the agent are in law ascribed to the principal.'[187] This would rest on an implied manifestation of assent that the primary wrongdoer should act on behalf of the secondary actor insofar as he unlawfully causes loss to others.[188] However, not all secondary liability is relational: consider a website that procures infringement undertaken by users solely for their own benefit. The agency account is directly

---

[181] Tony Weir, *Economic Torts* (1997) 38.

[182] See, eg, *Torquay Hotel Co v Cousins* [1969] 1 All ER 522, 530 (Lord Denning).

[183] He who employs another to do it does it himself.

[184] See, eg, Stevens, above n 24 (ch 2), 244–6.

[185] *Lyon*, 564; 213 (Crompton J). See, more equivocally, *Launchbury v Morgans* [1973] AC 127, 135 (Lord Wilberforce).

[186] Stevens, above n 24 (ch 2), 245.

[187] *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153, 198–9 (Lord Diplock).

[188] See Peter Watts (ed), *Bowstead & Reynolds on Agency* (19th ed, 2010), [1-001]; Gerard McMeel, 'Philosophical Foundations of the Law of Agency' (2000) 116 *Law Quarterly Review* 387, 389–90, 410–11.

contradicted by more modern authorities, which impute *liability* for the wrong of the primary wrongdoer.[189]

Further, it cannot be that *acts* constituting primary wrongdoing are literally attributed to joint tortfeasors; otherwise there would be *two* sets of tortious acts and two torts. Instead, 'if one party procures another to commit a tort … both are the principal wrongdoers *of the same tort*'.[190] Given that there is a single tort, it must be that joint tortfeasors are liable separately and together for the same act of wrongdoing, rather than liable for the notional acts of two people. This explains the requirement that the secondary actor must 'make the *wrong* his own'. If the acts were already his own, this addition would be superfluous. The better answer is that a claimant's rights in tort against one wrongdoer extend to any secondary actors who adopt the primary wrongdoer's acts as their own. Secondary liability rules merely recognise that we are all under sub-duties — to avoid inducing, granting authorisation or conspiring with others to commit wrongs — as elements inherent in primary duties.[191]

(c) *Upholding primary duties*

A third set of justifications argues that secondary liability rules are necessary to protect the integrity of an underlying primary right, such as a promise, fiduciary relationship or property. Such rules prevent secondary actors from devaluing primary rights by removing pre-emptive reasons for compliance. This ensures that moral lacunae do not arise where morally culpable parties interpose 'innocent' intermediaries. Thus, Lord Hoffmann described *Gye* as a doctrine which 'treats contractual rights as a species of property *which deserve special protection*'.[192] Secondary liability is said to 'strengthen',[193] 'extend'[194] or 'reinforce' duties owed by primary actors, thereby protecting the claimant's primary interest in performance. The problem with this account is that these doctrines operate (as has been argued) throughout private law, so it cannot be said that a single species of right is singled out for 'special protection' — except, perhaps, fiduciary duties. Moreover, the added protection afforded by secondary remedies is incomplete;

---

189 *Majrowski v Guy's & St Thomas's NHS Trust* [2007] 1 AC 224, 229–30 (Lord Nicholls), 245 (Baroness Hale), 248 (Lord Brown).

190 *Credit Lyonnais*, 549 (Lord Woolf MR) (emphasis added).

191 Agency-based explanations are most useful in cases where authority is specifically delegated to a primary wrongdoer — something which internet intermediaries rarely do: cf Watts (ed), above n 188, [8-176].

192 *OBG*, 27 (Lord Hoffmann).

193 Davies, above n 20, 404, 409.

194 Carty, above n 49, 668.

for example, it would not make conceptual sense to require the secondary party to disgorge profits retained only by the primary wrongdoer.

(d) *Upholding duties voluntarily assumed*

Finally, secondary liability may be understood in terms of the responsibility which secondary wrongdoers assume for the actions of primary wrongdoers: for example, by helping, requesting, authorising, or ratifying them. To view secondary liability as premised upon an assumption of responsibility overcomes the basic objection that secondary liability rules interfere with a person's liberty by holding them accountable for conduct which is not theirs. As Bagshaw argues, there must be 'special reasons' for holding someone responsible for third parties' conduct.[195] Attribution is justified where responsibility stems from a person voluntarily undertaking an obligation which can properly be upheld.[196] Secondary liability may actually promote the concept of individual responsibility and the purposes of tort law since it enforces secondary wrongdoers' duties to control primary wrongdoers with whom they share a nexus of causation and responsibility.[197] (There is obvious overlap with category (a) above.)

This account must be clarified in two ways. First, it will often be the case that a secondary wrongdoer wishes to avoid rather than assume responsibility for the primary wrongdoing; accordingly, the responsibility assumed is here notional — it reflects an expectation imposed by tort law having regard to the secondary wrongdoer's conduct, knowledge and control. The further riposte, that this simply involves 'a policy of conscripting "controllers" into the ranks of [tort] prevention authorities',[198] can be met by observing that those who facilitate harm play a part in violating the claimant's rights. While this may in itself be insufficient for monetary liability, it justifies some level of blame. As Cane argues, wilful disregard for primary rights justifies restricting secondary actors' choices by imposing liability:[199] the choice to be involved in others' wrongful conduct forfeits any initial right of moral autonomy they once enjoyed. Second is the charge of circularity: to say that the secondary actor is liable because she owes (or has assumed) a duty of care for the primary wrongdoer's actions begs the question, since whether such a duty exists is the very issue to be determined. Ultimately, the answer is a function of tort law

---

[195] Roderick Bagshaw, 'Inducing Breach of Contract' in Jeremy Horder (ed), *Oxford Essays in Jurisprudence* (2000) 131, 148.

[196] See J C Smith and Peter Burns, '*Donoghue v Stevenson* — The Not So Golden Anniversary' (1983) 46 *Modern Law Review* 147, 157. See also *Stovin v Wise*, 935 (Lord Nicholls).

[197] See, by analogy, McIvor, above n 171, 159.

[198] Smith, above n 177, 44–5.

[199] Peter Cane, '*Mens Rea* in Tort Law' (2000) 20 *Oxford Journal of Legal Studies* 533, 546.

more generally: duties may be assumed expressly — for example, by conducting risk-taking activity,[200] giving advice[201] or exercising control[202] — or by satisfying a connecting factor sufficient for secondary liability.

3.2 Practical functions

Consequentialist justifications of secondary liability argue that it promotes efficient internalisation of wrongdoing, thereby deterring wrongs and lowering both individual and overall enforcement costs. While this section does not defend these distributive arguments as valid normative justifications of secondary liability, it does identify three plausible descriptive accounts: reducing claimants' enforcement costs by conscripting least-cost avoiders; encouraging innovation; and regulating communications policy. These parallel streams inform and are shaped by the considerations of fault and personal responsibility considered above.

(a) *Reducing claimants' enforcement costs*

Enforcement against secondary parties is cheaper than suing primary wrongdoers if the aggregate costs of identifying each primary wrongdoer, proving liability and recovering judgment outweigh the total costs of recovery against enabling intermediaries. Without a way to target facilitators, inducers and conspirators, claimants face the Sisyphean task of suing every tortfeasor. Moreover, without the cooperation of secondary actors, claimants may lack the information necessary even to identify them. To solve this problem, doctrines of secondary liability create 'gatekeeper' regimes, allowing claimants to exploit natural enforcement bottlenecks and reduce overall costs.[203] The function of secondary liability is to set default rules where high transaction costs would otherwise prevent optimal private ordering between claimants and wrongdoers. Such rules encourage intermediaries to internalise the cost of negative externalities their services create — for example, by using contractual mechanisms to allocate liability to primary wrongdoers, increasing service prices or policing wrongdoing.[204]

---

[200] See Harrison Moore, 'Misfeasance and Non-feasance in the Liability of Public Authorities' (1914) 30 *Law Quarterly Review* 276, 278.

[201] See, eg, *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465, 494–5 (Lord Morris), 487 (Lord Reid).

[202] See, eg, *Dorset Yacht*, 1030 (Lord Reid).

[203] See Kraakman, above n 46 (ch 2), 56.

[204] Lichtman and Posner, above n 45 (ch 1), 229–30.

This has two consequences: first, it increases the net value of primary rights, with corresponding increases in any social benefits which those rights were designed to incentivise (for example, the creation of beneficial works); and second, it deters primary wrongdoing, which may reduce related social harms (for example, by increasing the quality of speech). The threat of liability incentivises secondary actors to act in ways that reduce total costs and increase net savings to society — in other words, to act as least-cost avoiders — just as the tort of negligence conditions liability for accidents upon a failure to take optimal precautions.[205] In aggregate, this is said to reduce the cost of preventing and correcting breaches of primary obligations. Consequentialists regard secondary liability as appropriate only when these benefits outweigh its costs, such as lost positive externalities caused by restricting non-tortious conduct.[206] However, those costs can elude quantification where they produce indirect harms to 'soft' interests such as freedom of expression, innovation and privacy.

Insofar as it offers a descriptive account, this view is difficult to reconcile with the fault-based requirements for causative secondary wrongdoing in English law. As Mann and Belzley argue, true efficiency-based secondary liability 'should have nothing to do with a normative assessment of the … intermediary' — whether the secondary actor behaved ignorantly, dishonestly or blamelessly — since its sole criteria are the relative costs and effectiveness of enforcement.[207] Yet even least-cost avoiders are not liable unless they have intentionally induced, dishonestly assisted, authorised or conspired in wrongdoing. This reflects the reasonable assumption that ignorant intermediaries are often unable to prevent wrongdoing without high social costs; fault is, in other words, a good heuristic for efficient loss avoidance. However, it means that English and European law are not *solely* concerned with efficient detection and prevention of primary wrongdoing; indeed, in *eBay*, secondary liability was refused notwithstanding the Court's conclusion that eBay *could* feasibly do more to prevent wrongdoing. Conversely, courts have all but ignored the liability of payment intermediaries, which might — as suggested in chapter 7 — be very efficient regulators of primary wrongdoing. Efficiency cannot account for these additional normative thresholds and therefore offers only a partial explanation of these doctrines' aims.

---

[205] See Guido Calabresi, *The Costs of Accidents: A Legal & Economic Analysis* (1970); Stephen Gilles, 'Negligence, Strict Liability and the Cheapest Cost-Avoider' (1992) 78 *Virginia Law Review* 1291.

[206] See William Landes and Richard Posner, *The Economic Structure of Intellectual Property Law* (2003) 118–19; Lichtman and Posner, above n 45 (ch 1), 238–9.

[207] Mann and Belzley, above n 52 (ch 1), 265.

(b) *Encouraging innovation*

Consequentialists explain safe harbours as mechanisms for ensuring that secondary liability is imposed upon intermediaries only when they are least-cost avoiders. They help efficiently apportion liability between primary and secondary wrongdoers by creating incentives for intermediaries to adopt low-cost procedures to remove material for which litigation is disproportionately costly, while recognising that intermediaries are unlikely to be least-cost avoiders unless they are actually aware of wrongdoing.[208] In other words, although *ex ante* monitoring may carry excessive social costs, intermediaries are usually more efficient at *ex post* removal than primary wrongdoers.[209] When Parliament or courts intervene to impose or limit secondary liability, they use a retrospective mechanism to shift innovation and dissemination entitlements between incumbent industries and technological innovators. These interventions reflect an assessment of net social welfare that seeks to induce the inefficient party to internalise the cost of wrongdoing and so avoid future inefficient investments.[210]

Safe harbours also provide bright lines and clear zones of activity within which intermediaries may act without fear of potential liability.[211] In supplying clear guarantees of immunity, they reduce uncertainty and (at least in theory) facilitate investment in new technologies. Further, they reduce the need for secondary actors to make decisions about primary wrongdoing, which reduces the risk of pre-emptive over-enforcement.[212] Intermediaries might otherwise do so because they do not internalise the benefits of tortious activity or incur the social costs of excessive enforcement.[213] For courts, these limits function as liability heuristics, reducing decision costs and ultimately the cost of supplying internet services to consumers — all of which encourages investment and innovation. However, safe harbours may not go far enough, since the marginal utility derived from servicing primary wrongdoers may lead intermediaries to abandon 'risky subscribers'.[214] Innovation-based accounts therefore acknowledge that the limits of secondary liability embody a compromise between strict and fault-based responsibility that reflects wider considerations of social policy and market forces.

---

[208] Rustad and Koenig, above n 89 (ch 1), 391.

[209] European Commission, *Report on the Application of Directive 2004/48/EC* (22 December 2010) 9.

[210] Dotan Oliar, 'The Copyright–Innovation Tradeoff: Property Rules, Liability Rules, and Intentional Infliction of Harm' (2012) 64 *Stanford Law Review* 951, 1001.

[211] Lichtman and Landes, above n 63 (ch 1), 406.

[212] Mann and Belzley, above n 52 (ch 1), 274.

[213] Assaf Hamdani, 'Gatekeeper Liability' (2003) 77 *Southern California Law Review* 53, 73. Cf Lichtman and Posner, above n 45 (ch 1), 225–6.

[214] Neal Katyal, 'Criminal law in Cyberspace' (2001) 149 *University of Pennsylvania Law Review* 1003, 1007–8.

(c) *Regulating communications policy*

Finally, legal realists identify the wider role of secondary liability rules in regulating access to information. Secondary actors are natural targets for propagating communications policy and enforcing rights in and against information, since they have always been gatekeepers crucial for its reproduction and dissemination.[215] Those policies serve numerous purposes, from preserving existing business models and protecting incumbent industries, to minimising consumer search costs.[216] Secondary liability rules are one method of regulating the interface between each generation of disseminating industries and those with an interest in what is being disseminated. They appoint judges as technological gatekeepers who assess the likely harms and benefits of new entrants' technologies, deciding whether, on balance, they should be immunised or face extended liability.[217] Following this assessment, Parliament may intervene to reverse or codify an emergent policy.

That tort law specifies high thresholds for secondary liability reflects an underlying policy of entrusting regulation to market forces unless the harms of new technology *clearly* outweigh their benefits. Safe harbours partially codify these policies. If they are pragmatic compromises, this reflects the contested nature of modern communications policies.[218] This approach views the limits of secondary liability as an evolving battleground of regulation which corrective theory cannot wholly explain; although principles of tortious responsibility inform doctrines of secondary liability, they are subservient to a Kronosian cycle of innovation, market disruption and regulation in which courts and Parliament periodically rebalance wider interests of competition and economic policy, human rights, innovation, regional and international trade policy,[219] and the complex incentive structures underlying primary legal norms.

---

[215] Wu, above n 32 (ch 1), 712–13.

[216] See, eg, Stacey Dogan and Mark Lemley, 'Trademarks and Consumer Search Costs on the Internet' (2004) 41 *Houston Law Review* 777, 795–7, 831.

[217] See Wu, above n 60 (ch 1), 348–9, 364.

[218] Ibid 356.

[219] See Graeme Dinwoodie, 'The WIPO Copyright Treaty: A Transition to the Future of International Copyright Lawmaking' (2007) 57 *Case Western Reserve Law Review* 751, 757–8 (it might be added that intermediaries now represent a 'fourth vector' of balance in the post-*ACTA* calculus).

4 Conclusion

This chapter has identified a class of doctrines which impose secondary liability upon derivative wrongdoers whose conduct meets certain causal and normative thresholds. These thresholds are rarely met by passive and neutral intermediaries, which (despite causing harm) usually lack the required knowledge and intention. Limitations derived from European law further entrench the principle that faultless intermediaries should not face monetary liability or onerous duties to police third parties' wrongdoing.

This chapter concluded by considering two sets of justifications for imposing secondary liability. The first sought to bring secondary wrongdoers' liabilities within traditional accounts of personal responsibility in tort. This chapter argued that they can be best explained by secondary wrongdoers' assumption of responsibility for primary wrongdoers. The second set of justifications invoked the language of law and economics to explain why certain secondary actors are appropriate targets of loss-shifting. Although economic analysis provides a powerful vocabulary to describe the communications policy underlying secondary liability rules, the agnosticism of enforcement cost analysis offered few clear answers to underlying questions of fault, responsibility and fundamental rights.

The high thresholds of knowledge and intervention required for secondary liability suggest that these rules are unlikely to be effective at regulating internet intermediaries alone. In the next part, this research considers the application of doctrines of tortious and statutory secondary liability to intermediaries in defamation (chapter 4) and copyright (chapter 5) actions. These chapters develop the argument that monetary liability rules have failed to offer effective relief to claimants and balance intermediaries' and users' interests fairly.

4
Defamation

Fuelled by the scale, ubiquity and permanence of internet content, and by the public's appetite for scandal and intrigue, online defamatory statements possess unparalleled potential to harm a person's reputation indelibly. Necessarily, when such statements are promulgated, it is an intermediary which processes, stores and transmits them. This chapter considers when such a party is liable to pay damages to the claimant. This question is, in one sense, far from new: similar concerns have attended the arrival in England of less advanced tools for mass communication

since at least 1476.[1] Partly in response to those concerns, tort law has long recognised the potential for innocent messengers, distributors and other secondary parties to face liability on the basis that, although they are not the primary authors of defamatory material, they have 'taken part' in its publication.[2] Simultaneously, the concept of publication has developed built-in limits which exonerate services that supply only the means or facilities of publication, while various statutory enactments have further limited secondary liability.

The purpose of this chapter is not to attempt an exhaustive study of the English law of defamation or its history, but rather to analyse the development and application of doctrines of secondary liability in disputes involving the defendants identified in chapter 2. Section 1 traces the evolution of 'publication' in actions involving intermediaries, observing that the concept has functioned as a flexible — but not always unambiguous or coherent — lever for upholding various political and regulatory policies concerning the dissemination of information, while its breadth has left little room for doctrines of joint tortfeasorship. Section 2 analyses recent actions against internet intermediaries, concluding that *prima facie* liability now depends upon actual or implied authorisation, approval or acquiescence in the defamatory words. Section 3 identifies and defends statutory limitations on liability, which reflect a policy of encouraging complainants to resolve disputes directly with the author, editor or primary publisher of the impugned material. Despite sometimes lacking clarity, those limitations strike an appropriate balance between reputation, innovation and freedom of expression. However, to ensure adequate protection for claimants, section 4 proposes several complementary non-monetary orders such as identity disclosure, alternative dispute resolution, and discursive remedies.

1 The scope of secondary liability for defamation

1.1 The publication requirement

An essential element of any claim in defamation is that the defendant has published or participated in the publication of defamatory material.[3] This requires the claimant to prove two matters: first, that the material was communicated to at least one other person; and, second, that the defendant was in law responsible for the act of communication.[4] Communication can occur using any means

---

1 See Colin Lovell, 'The "Reception" of Defamation by the Common Law' (1962) 15 *Vanderbilt Law Review* 1051, 1062 (describing the arrival of the Caxton press at London).

2 This discussion ignores cases where an intermediary (or its employee or agent) is the originating author, editor or publisher, such conduct being primary wrongdoing: see chapter 3, § 1.1.

3 See *Broughtons Case* (1583) 1 Moo KB 141; 72 ER 493.

4 See *Edwards v Wooton* (1608) 12 Co Rep 35; 77 ER 1316; *Jones v Davers* (1653) 1 Cro Eliz 497; 78 ER 747; *Barrow v Lewellin* (1792) 1 Hob 62; 80 ER 211.

through which it is possible to impart information, whether in a conventional analogue medium — such as speech or printed text — or an electronic one — such as a computer network or broadcast.[5] The existence of the communication requirement is consistent with the modern view that the gist of defamation lies not in the mere saying or writing of words, but in their actual conveyance to others, in whose eyes the claimant's reputation is lowered.[6]

The traditional basis of liability for defamation is that each person who 'takes part' in a publication of defamatory material is, subject to any available defences, a joint tortfeasor and liable to compensate the claimant, regardless of the degree of participation.[7] In well-settled areas — for example, communications by the author,[8] editor,[9] trade publisher or printer[10] of material — publication is rarely in doubt. However, as will become apparent, judicial definitions of 'taking part' provide very limited guidance in determining whether a party is responsible for communicating defamatory material in borderline cases, instead offering only vague conclusions, frequent contradictions, and an unhelpful tendency towards metaphor and simile. For this reason, adducing clear indicia of intermediary publication is a task of considerable difficulty.

1.2 Publication by intermediaries

At common law, the liability of intermediaries has closely paralleled judicial refinement of the classes of person regarded as publishers. This process has, in turn, been informed by a wide range of historical and political factors, from the suppression of duelling[11] and the regulation of political and religious speech,[12] to jurisdictional competition between common law, Star Chamber and ecclesiastical courts.[13] Although a comprehensive account of these factors is beyond the scope of this chapter, it proves instructive to consider two aspects of this history: first, the striking manner in which the concept of publication has accommodated rapid changes in the technology used to print and disseminate defamatory material; and second, the development of a fault requirement

---

5 *Al Amoudi v Brisard* [2007] 1 WLR 113, 121–2 (Gray J); *Totalise* (discussed below in chapter 7).

6 *Pullman v Hill & Co* [1891] 1 QB 524, 527 (Lord Esher) (a man cannot publish to himself); *Powell v Gelston* [1916] 2 KB 615, 619 (Bray J) (publication 'is the foundation of the action').

7 David Price and Korieh Duodu, *Defamation Law, Procedure & Practice* (3rd ed, 2004) [3-02].

8 *Bond v Douglas* (1836) 7 C & P 626.

9 *Watts v Fraser* (1835) 7 C & P 369.

10 *Goldsmith v Sperrings Ltd* [1977] 1 WLR 478, 487 (Lord Denning MR).

11 *Lord Darcy v Markham* (1792) 1 Hob 120, 121; 80 ER 270 (attempt to provoke a duel using slanderous words).

12 See Holdsworth, *A History of English Law* (1926) vol 8, 336.

13 See *Palmer and Thorpe's Case* (1583) 4 Co Rep 20a (Lord Coke); Roscoe Pound and Theodore Plucknett, *Readings on the History and System of the Common Law* (3rd ed, 1927) 71–2, 480.

for secondary disseminators. This section traces those themes in relation to four classes of offline intermediaries: (1) operators of printing presses; (2) innocent disseminators of printed libels; (3) owners of property on which defamatory matter is exhibited; and (4) postal and telegraphy services. These cases are the source of most analogies used in internet defamation cases.

(a) *Printers*

The difficulty of acquiring and concealing early printing presses made them natural targets for the suppression of unwanted political speech.[14] Criminal prosecutions for seditious libel provided one of several options for regulating gatekeepers of printing technology.[15] For example, *R v Knightly* was a Star Chamber prosecution against a Member of Parliament who had allowed reformists to use his hidden press for the purpose of printing libellous pamphlets.[16] At this time, both the operator and proprietor of the press were strictly liable for the resulting publications, regardless of whether they had seen, produced or authorised their contents. *R v Clerk* provides an extreme example, where a printer's servant was convicted of criminal libel, though he could not read what was being printed and his only involvement was to 'clap down' the press at the direction of his employer.[17] His ignorance and limited contributions were 'entirely immaterial', since to publish did not require malice — merely that the defendant caused printing to occur. Political expediency, in short, demanded absolute liability.

The scope of publication mirrored advances in printing technology and practice. In *Baldwin v Elphinston*,[18] the act of printing a libel onto paper was considered evidence of publication, since the defamatory material was delivered to the print compositor and workmen who operated the presses. A century later, technology had evolved to the point where secondary parties no longer needed to be involved, and the inference was abandoned in *Watts v Fraser*.[19] These changes made it increasingly difficult to prove publication, and seditious libel — like the systems of censorship, taxation and print licensing that preceded it — became ineffective as a means of controlling private printing. The combined effect of unfavourable precedent, changes in public opinion and wider

---

[14] Van Vechten Veeder, 'The History and Theory of the Law of Defamation' (1904) 4 *Columbia Law Review* 33, 45.

[15] Other options included treason, *scandalum magnatum*, heresy and the systems of royal and statutory print licensing: see Philip Hamburger, 'The Development of the Law of Seditious Libel and the Control of the Press' (1985) 37 *Standard Law* Review 661, 666–73.

[16] (1588) 31 Eliz 1263.

[17] (1744) 1 Barn KB 304, 305; 94 ER 207.

[18] (1775) 2 Blackstone W 1037, 1038; 96 ER 610, 611 (De Grey CJ).

[19] (1837) 7 Ad & El 223, 232; 112 ER 455, 460 (Lord Denman CJ).

access to printing presses was to force governments to target intermediaries in other ways, as previous regulatory strategies 'became inadequate, defunct, or otherwise obsolete.'[20]

Both printers and proprietors of newspapers were strictly liable for publishing others' defamatory material.[21] In *Zenger's Case*, Lancey CJ justified secondary liability by conjuring the spectre of an illiterate intermediary, who could be employed 'to publish the most virulent papers with the greatest security'.[22] Later, in *Dixon v Enoch*,[23] the Court accepted that separate civil actions might lie against the printer, trade publisher and proprietor of the *Pall Mall Gazette* regardless of their knowledge of the defamatory matter it contained.

(b) *Disseminators*

Circulators and distributors of defamatory material may also be publishers. Early cases imposed strict liability. *R v Harris*, for example, records the conviction of a bookseller at Guildhall for selling a blasphemous book, despite his ignorance of its contents.[24] By the close of the 19th century, distribution liability had undergone a dramatic transformation: it required fault. The seminal case was *Emmens v Pottle*,[25] in which the defendant newsvendors were circulators of a newspaper which defamed the claimant. The jury found the defendants blameless, since they were neither aware of the libels nor negligent in their ignorance. Dismissing the claimant's appeal, Lord Esher MR explained that a secondary disseminator, although *prima facie* liable as a publisher, will be exonerated if it exercises reasonable care yet lacks knowledge of the defamatory character of material. This reflected two differences between primary and secondary disseminators: first, the original author, printer or proprietor brought the libel into existence and thereby assumed some responsibility for it; and, second, extending strict liability to disseminators would carry oppressive social consequences, since

> the result would be that every common carrier who carries a newspaper which contains a libel would be liable for it, even if the paper were one of which every man in England would say that it was not likely to contain a

---

[20] Hamburger, above n 15, 761.

[21] Cf *Lobay v Workers and Farmers Publishing Association* [1939] 2 DLR 272, 275 (Taylor J) (the defendant printer knew its equipment was being misused and failed to do anything about it); Atiyah, above n 51 (ch 2), 297 (preferring to view *Lobay* as an example of joint 'assistance' liability).

[22] *R v Zenger* (1735) 9 Geo II 675, 677 (emphasis added).

[23] (1871) 8 LR 394, 399 (Wickens VC).

[24] (1680) 32 Charles II 925, 930. See also *R v Curll* (1727) 17 St Tr 154.

[25] (1885) QBD 354 ('*Emmens*').

> libel. To my mind the mere statement of such a result shews that the proposition from which it flows is unreasonable and unjust.[26]

The meaning of negligent publication was considered further in *McLeod v St Aubyn*,[27] where the alleged publication was the appellant handing to a librarian an unread copy of a newspaper in which certain scandalous material appeared. The Privy Council accepted that the appellant was not a publisher of the newspaper but a 'mere agent and correspondent of it'.[28] Failing to read the newspaper before handing it on was not negligent because the appellant, unlike a printer or publisher, 'never intended to publish' the material. Although this was a criminal prosecution for contempt of court, *McLeod* is consistent with the general principle that fault is required to publish words (unlike for their composition): if a defamatory statement is communicated accidentally or inadvertently by a party, there will not be publication.[29]

Similarly, in *Bottomley v F W Woolworth & Co Ltd*, a supermarket was not a secondary publisher of articles in an American magazine which it distributed on consignment.[30] Although the supermarket did not employ anyone to read what it sold, there was no reason to suspect that the magazine contained libels and its dissemination was not negligent. Conversely, in *Vizetelly v Mudie's Select Library Ltd*,[31] the proprietors of a circulating library that lent out a defamatory book were liable for publishing that material. Smith LJ held that the defendants' ignorance of the libel was for want of care: the library did not employ anyone to examine books, did not take heed of publishers' circulars, and had admitted that it was cheaper to be sued for libels than examine each book.[32] This outcome is difficult to reconcile with *McLeod*, *Emmens* and *Woolworth*,[33] where the disseminators were held to much lower standards of care.

The 20th century saw growing reluctance to impose liability on commercial distributors. This reluctance is particularly evident — though ultimately not triumphant — in *Goldsmith v Sperrings Ltd*,[34] where a prominent businessman alleged that he had been defamed by three articles appearing in *Private Eye*. In addition to suing the proprietor, editor and wholesale distributor of the magazine, he commenced proceedings against 37 secondary distributors, including the defendant, a Southampton newsagency. It was not alleged that they had done anything wrong

---

26 Ibid 357 (Lord Esher MR) (Cotton LJ agreeing). See also ibid 358 (Bowen LJ).

27 [1899] AC 549 ('*McLeod*').

28 Ibid 562 (Lord Esher MR).

29 *Huth v Huth* [1915] 3 KB. Cf *Weld-Blundell v Stephens* [1920] AC 956 (negligent publication).

30 *Bottomley v F W Woolworth & Co Ltd* (1932) 48 TLR 521 ('*Woolworth*'); approved in *Tamiz (CA)*, [26].

31 [1900] 2 QB 170.

32 Ibid 175–6 (Smith LJ). See also ibid 178 (Vaughan Williams LJ), 179 (Romer LJ).

33 See also *Weldon v 'The Times' Book Company (Ltd)* (1911) 28 TLR 143.

34 [1977] 1 WLR 478 ('*Goldsmith*').

other than distribute *Private Eye*. The majority adopted the traditional view, which went undisputed by counsel, that distributors of the magazine were *prima facie* liable, subject to the defence of innocent dissemination. On this basis, their Lordships refused to strike out the proceeding as an abuse of process.

However, in a strong dissent, Lord Denning MR argued that the onus of proof should be reversed, so that distributors are not liable unless the claimant proves they have actual or constructive notice of the libel. Although *Private Eye* had a reputation for controversy, this was not enough to fix the defendant with knowledge of the *likelihood* of a libel. Disseminators of newspapers

> are *nothing more than conduit pipes in the channel of distribution. They have nothing whatever to do with the contents.* They do not read them … Common sense and fairness require that no subordinate distributor … should be held liable … unless he knew or ought to have known that the newspaper … contained a libel[35]

This approach alludes to Lord Sumner's metaphor of 'mere conduits'. Even *prima facie* liability would risk stifling freedom of the press and its 'channels of distribution'.[36] Lord Denning's appeal to principles of fairness reflects an implicit claim that carriers who are oblivious to what they are charged with carrying and incapable of knowing otherwise are blameless for going about their business. Without a reasonable possibility to detect wrongdoing, the carrier could not avert it and would probably not be a least-cost avoider. This is especially true of a tort which does not require intent to defame or knowledge of a statement's falsity: a carrier could otherwise face liability despite reasonably believing a statement to be true or justified.

(c) *Property owners*

Liability can arise simply by exhibiting defamatory matter, whether or not it was authored by the exhibitor.[37] *Byrne v Deane* provides the well-known example of a golf club proprietor who was liable for publishing a defamatory poster which an unknown patron had affixed to its wall.[38] The Court reasoned that publication could be inferred from the club's failure to remove the material where it: (1) had actual knowledge of the material; (2) exerted control over the material (in the sense of the ability and authority to remove it); and (3) knew that the material would, if not

---

[35] Ibid 487 (Lord Denning MR) (emphasis added).

[36] Ibid 488 (Lord Denning MR).

[37] *Buckley v Wood* (1591) 33 & 34 Eliz 888, 891; 4 Co Rep 14b. See also *Hersey's Case* (1572) 77 ER 1378; 12 Co Rep 103, 104 (damages awarded for exhibition of a malicious bill).

[38] [1937] 1 KB 818, 830 ('*Byrne*').

removed, be communicated to patrons of the club who saw it. In those circumstances, Greene LJ held that:

> The proper inference … is that [the proprietors] were consenting parties to its continued presence on the spot where it had been put up. That being so … they must be taken to have consented to its publication to each member who saw it.

Liability in *Byrne* was founded on an inference of 'consent to publication' arising from the defendant's culpable acquiescence in the libel. It follows that an exhibiting intermediary will face liability for its failure to prevent a third party publication only in the limited circumstances where it exercises control over the facilities or premises through which publication occurs and the defendant is aware of that publication. To the extent that this conduct is also an example of 'taking part' in publication, *Byrne* suggests that participation is strongly related to an intermediary's knowledge, control and foresight of wrongdoing.[39] This is difficult to reconcile with the traditional requirement that publication be wilful, which arguably precludes liability for publications by omission. Such cases are therefore better understood as instances of secondary liability by authorisation.[40]

(d) *Postal and delivery services*

Parties who deliver defamatory articles are *prima facie* liable for publications to the recipient. However, they escape liability upon proof that at all times they lacked knowledge that the contents were defamatory. In *Day v Bream*, the porter of a London coach office was not liable for delivering bundles of defamatory handbills to inhabitants of the building, because the defendant could 'shew his ignorance of the contents'.[41] Patteson J accepted that delivery raised a *prima facie* presumption of publication, but this was rebutted where the defendant conveyed the parcels innocently, 'in the course of his business without any knowledge of their contents'. It is unclear whether 'the contents' of handbills refers to the words used, their defamatory character, or their actionability. Mitchell takes a broad view, arguing that 'knowledge that his action *would injure the claimant's reputation* was crucial';[42] on this view, the disseminator would escape liability without at least awareness that the words used were defamatory. Arguably, this does not go far enough, since it fails to consider the availability of defences which render a defamatory statement justified;

---

[39] See also *Urbanchich v Drummoyne Municipal Council* (1991) Aust Tort Rep 81-127 (public authority liable for defamatory posters exhibited in bus shelters by members of the public).

[40] See below § 1.3.

[41] *Day v Bream* (1837) 2 M & R 54, 56; 174 ER 212 (Patteson J).

[42] Paul Mitchell, *The Making of the Modern Law of Defamation* (2005) 107 (emphasis added).

however, because it will ordinarily be impossible for a delivery agent to read, much less assess the veracity of words contained in a package, the effect may often be the same. Like other qualifications upon dissemination liability, this result sits uncomfortably with the orthodox view that publication does not depend on the defendant's knowledge of the specific words used. If communication is constituted by delivery, it is difficult to see how the deliverer's mental state can transform that act into something other than a publication. *Day v Bream* is therefore better characterised as an early example of the defence of innocent dissemination.[43]

1.3 Joint tortfeasorship

Just as a defamation may be carried out jointly by A and B as co-authors or joint distributors,[44] it may also be perpetrated where A procures or joins in a common design with B to publish defamatory material. Under the general principles of joint tortfeasorship examined in chapter 3, A will be liable despite not herself communicating the material. This liability is secondary rather than primary because it derives from, and intrinsically depends upon, B's independent wrong of publication. While there are no conceptual barriers to applying this approach in defamation cases, in practice publication has proved sufficiently flexible that secondary liability rules have normally been unnecessary. Instead, there are a series of publications effected by parties who, while acting jointly, also 'take part' as primary common law publishers.[45]

Some 19th century cases refer to the liability of one who authorises another to publish defamatory material.[46] An authoriser is said to be a publisher of the material, which suggests that her liability is primary. However, because the authoriser does not herself engage in the act of communication, this is an example of secondary liability deriving from the authorised party's act of communication. In *R v Cooper*, the defendant was liable for approving a defamatory article published by a newspaper, where there was 'substantial identity' between what he authorised and what the newspaper later published.[47] The test was simply whether the defendant 'approved of' something which was defamatory and furnished the necessary material. Likewise, *Byrne*'s emphasis on 'consent' to a publication may be characterised as an example of secondary liability arising from an *implied* approval of the published material, where the approval is inferred from

---

43 Later cases appear to take this view: see *Ridgway v Smith & Son* (1890) 6 TLR 275; *Mallon v W H Smith & Son* (1893) 9 TLR 621.

44 Williams, above n 26 (ch 3), 10.

45 See, eg, Lord Porter et al, *Report of the Committee on the Law of Defamation* (1948) (Cmd 7536) 29.

46 See also *Webb v Bloch* (1928) 41 CLR 331, 364 (Isaacs J).

47 (1846) 8 QB 533, 536 (Lord Denman CJ), 537 (Coleridge J).

silence coupled with knowledge and control. More recently, Tugendhat J considered it a live issue whether employees who had spoken allegations to the defendant had thereby 'authorised' him to publish the material to a journalist.[48]

Similarly, a request to publish defamatory material can be sufficient for liability, but not a 'mere wish or hope'.[49] The purpose is to prevent a party from deploying 'the safe shelter of intermediate agents.'[50] However, these cases are probably better dealt with as examples of joint tortfeasance, since a request would be procurement. Ultimately, the absence of modern cases on secondary liability suggests that it is an unnecessary gloss on publication, which is already sufficiently broad to encompass anyone who intentionally takes part by a request, permission or material contributory act.

2 Application to internet intermediaries

Defamation litigation against internet intermediaries has centred on two main issues: first, whether the defendant is a 'publisher' of defamatory material authored by a third party but cached, stored or transmitted using its services; and second, whether the defendant's activities attract the operation of a defence or statutory immunity. This section addresses the first question in light of how the English authorities have refined the concept of publication in internet defamation actions. It commences by examining claims against platform operators, before moving to parties further removed, such as hosts, ISPs, and gateways.[51] It identifies several emerging limits to the scope of publication which fully insulate network-layer intermediaries from liability and provide partial protection to application-layer services. The issue of defences is considered in section 3.

2.1 Platforms

Considering the volume of internet material published by intermediaries, surprisingly few cases address platforms' liability for third party statements. The majority of claims in this category instead concern material originating from website operators themselves — frequently journalists or bloggers — or their agent or employee. These claims do not concern us here since they are

---

48 *Hays plc v Hartley Ltd* [2012] EWHC 1068 (QB), [14] (Tugendhat J) ('*Hays*').

49 *Parkes v Prescott* (1869) LR 4 Exch 169, 179 (Montague Smith J).

50 Ibid 177, 179 (Montague Smith J).

51 Because defamation requires the conveyance of human-readable information, it implicates higher-layer services rather than physical-layer intermediaries.

determinable by established principles of primary and vicarious liability.[52] Other claims raise issues of internet publication incidentally, such as where the same material is published both in print and online.[53] The few claims against true secondary publishers involve user-created content posted to weblogs and discussion fora.[54] The factual and technical distinctions between platforms, and their varying levels of involvement in the conveyance of defamatory matter, underscore the importance of treating publication as a question of fact that examines the conduct of each defendant in the particular circumstances of the case. In these cases, three issues commonly arise: whether the information has been sufficiently published at all; whether the intermediary participated in publication; and the redisplay of archived material.

(a) *Proof of substantial publication*

To prove publication on a platform, the claimant must now establish that the defamatory statement has been intelligibly perceived by a substantial number of people within the jurisdiction besides the claimant.[55] This extension of the traditional publication threshold does not owe its existence to any unique property of the internet, but rather to s 6 of the *HRA* and the need for courts to balance the claimant's right to reputation against the defendant's freedom of expression. This is achieved by precluding trivial claims and other disproportionate demands on judicial resources.

Substantial local publication can sometimes be inferred from search engine visibility,[56] but normally requires proof of access rather than the mere potential for access. In *Loutchansky*, Gray J refused to infer publication of a headline story without evidence of visitors, even where the website in question received 12.5 million monthly visits.[57] Limited publication may be inferred to 'followers' of a weblog (or, by analogy, a Twitter account),[58] members of a website 'of specialist interest',[59] those who comment upon the impugned article,[60] and, perhaps, RSS and social media subscribers. In short, the question of website publication is answered in much the same manner

---

[52] See above ch 3, § 1.1.

[53] See, eg, *Atlantis World Group of Companies NV v Gruppo Editoriale L'Espresso SPA* [2008] EWHC 1323 (QB), [19], [42] (Gray J) (parallel publication of article in magazine and website).

[54] For platforms such as Google's Blogger.com, see below § 2.2(b) (they do not operate but are rather hosts of the relevant websites).

[55] *Jameel*, 966 (Lord Phillips MR). See also below § 3.3(c) for discussion of abuse of process.

[56] *Steinberg v Pritchard Englefield* [2005] EWCA Civ 288, [21] (Sedley LJ).

[57] *Loutchansky v Times Newspapers Ltd [No 2]* [2001] EMLR 876, [14]–[15], [20] (Gray J).

[58] *Davison*, [24] (HHJ Parkes QC).

[59] *Trumm v Norman* [2008] EWHC 116 (QB), [36]–[37] (Tugendhat J).

[60] *Kaschke*, [95] (Stadlen J).

as publication in print. Just as substantial publication can no longer be presumed from the mere fact that material was printed by its author, it cannot be presumed from material being made available on the internet.[61] Echoing the transition from *Baldwin* to *Watts* in the 19th century, this reflects the growing maturity of the internet as a publication medium.

A trio of cases has considered publication on social networks. First, *Applause Store Productions Ltd v Raphael* concerned litigation between two former friends for defamatory statements made by one against the other on Facebook.[62] The words complained of appeared in fake Facebook profiles which contained various libels on the claimant and his business. Although Facebook was not alleged to be a publisher, it did remove the material voluntarily and gave disclosure under a *Norwich Pharmacal* order.[63] Publication was assumed. Second, in *Elsbury v Talbot* the Court accepted that defamatory 'tweets' posted to Twitter could be actionable publications.[64] Third, *Cairns v Modi* awarded damages for tweets alleging match-fixing by the claimant, a well-known cricketer. Although only about 65 people had seen the messages, the Court inferred substantial publication to the defendant's followers.[65] In upholding this award, the Court of Appeal noted the tendency of social networks to make scandalous stories "'go viral" more widely and more quickly than ever before'. This was a legitimate factor to be taken into account when assessing liability.[66]

(b) *Participation in publication*

Courts have struggled to articulate coherent principles for assessing when a website operator is a publisher of defamatory user-created content. Only three English cases appear to deal with such material.[67] In *Metropolitan International Schools Ltd v DesignTechnica Corp*,[68] the first defendant operated an online consumer electronics discussion forum in which postings were made by unknown third parties. It failed to remove these postings, which criticised the claimant's distance learning courses as fraudulent. In entering default judgment, Eady J noted that his order was

---

61 *Al Amoudi v Brisard* [2007] 1 WLR 113, 123 (Gray J).

62 [2008] EWHC 1781 (QB).

63 See below chapter 6, § 3.5.

64 (Unreported, High Court of Justice, 10 March 2011).

65 [2010] EWHC 2859 (QB), [20], [41] (Tugendhat J); [2012] EWHC 756 (QB),. [122]–[123] (Bean J).

66 [2012] EWCA Civ 1382, [27] (damages only).

67 In a fourth case, *Carrie v Tolkien* [2009] EWHC 29 (QB), the *defendant* posted a critical comment to the claimant's weblog, which the operator allowed to stand for some 22 months, leading to the unsurprising conclusion that she had consented to the defamation: ibid [17] (Eady J). As an acquiescence case involving primary authors rather than intermediaries, it is distinguishable.

68 [2009] EWHC 1765 (QB) ('*DesignTechnica*'). See below § 2.4 in relation to search engines.

probably unenforceable against the American operator, but concluded that a clam lay against it.[69] The second case, *McGrath v Dawkins*, concerned reviews and comments posted to the claimant's book product page on Amazon.co.uk.[70] The Court assumed publication in the claimant's favour but struck out the claims against Amazon because they were defeated by the storage safe harbour.[71]

Third, in *Kaschke v Gray* an allegedly defamatory article was contributed by the first defendant and automatically published on the homepage of a political weblog created and maintained by the second defendant, Mr Hilton. Hilton occasionally removed, edited or 'promoted' posts, but did not monitor the weblog and was unaware of the offending material until notified by the claimant, whereupon he removed it.[72] Hilton conceded that there had been a publication, but argued that he did not participate in it and, in any event, a defence applied. Stalden J refused to strike out the claim, but appears to have dealt with only the second of these arguments, instead assuming that Hilton was a publisher.[73] It is suggested that this conclusion is far from obvious. While Hilton provided the facilities of publication and had some control over what was posted, he was not aware of the defamatory posting or any prospect that it would be conveyed to others.[74] The facts are therefore readily distinguishable from the conditions expressed in *Byrne*. The only reasoning consistent with the Court's finding is that his dissemination of the posting was somehow negligent in a way that might preclude reliance on *Emmens* and *McLeod*. However, *Kaschke* offers no indication of what the applicable standard of care might be. Paradoxically, to infer publication so readily from the *capacity* or historical tendency to moderate tortious material discourages website operators from developing and using the systems best capable of removing harmful content.

As an application for summary judgment, *Kaschke*'s refusal to rule out publication does not signal a return to strict liability. However, it creates considerable uncertainty about the test for platform publication. Although the availability of safe harbours and defences may make the precise test a question of little practical significance, it is suggested that the cases are best understood as creating a fault-based liability rule premised upon the defendant's implied authorisation of publication. Prior to notification, the *Emmens* standard applies: operators could normally not be publishers if they were not otherwise aware of the words used or failed to act as a reasonable

---

69 Ibid [46] (Eady J).

70 [2012] EWHC B3 (QB) ('*Amazon*').

71 See below § 3.2(c).

72 *Kaschke*, [27]–[28], [84]–[85] (Stalden J).

73 Ibid [40]–[41] (Stalden J).

74 Ibid [102]–[103] (Stalden J).

website operator would — for example, in procuring unreliable content, determining editorial and moderation policies, or failing to exclude known abusive users. Following notification, the *Byrne* standard applies: the question is whether by his conduct the operator authorised, consented to or assumed responsibility for the conveyance of the relevant words. This could be evidenced by intentional actions taken to promote or highlight the material, but it would be rarely inferred from silence without actual knowledge that the words are actionable, control over the content and a reasonable opportunity to act. In applying well-established principles, such an approach offers greater certainty and consistency with the test for offline publication. Additionally, it protects diligent website operators, encourages efficient investments in content moderation systems, and discourages intermediaries from soliciting or acquiescing in obviously tortious postings with impunity.

Finally, although several cases have considered defamatory statements published on social networks, none has considered whether the social network is itself a publisher. It is suggested that the principles considered below should apply by analogy, since social platforms are essentially providing a passive hosting service for users' material.[75]

(c) *Liability for archived materials*

Traditionally, English law regarded a separate cause of action as arising with each successive communication of a defamatory statement by a website.[76] This position, which significantly disadvantaged intermediaries (who faced endless liability where an article was kept online in a digital archive),[77] was recently abolished by statute.[78]

2.2 Hosts

Early authorities suggested that, subject to defences, hosts were *prima facie* publishers of material once put on actual or constructive notice of its defamatory character. However, more recent cases appear to ask whether the host is secondarily liable for authorising publication in the manner recognised in *Byrne v Deane*. This section argues that network-layer facilitation by a host does not amount to publication whether before or after receiving actual notice of the defamatory words,

---

[75] See below § 2.2(b).

[76] See *Duke of Brunswick v Harmer* (1849) 14 QB 185; *Lewis v King* [2004] EWCA Civ 1329, [29]–[30].

[77] See *Times Newspapers Ltd [Nos 1 and 2] v United Kingdom* (European Court of Human Rights, Fourth Section, 10 March 2009) [45]–[49].

[78] Defamation Bill 2012 (UK) cl 8.

until the host's conduct (including a failure to act) would reasonably be regarded as an assumption of responsibility for or acquiescence in the primary wrongdoing.

(a) *Godfrey v Demon Internet Ltd*

Godfrey decided that a Usenet host is a publisher where: (i) material is uploaded to equipment under its control; (ii) the material is 'on its face defamatory'; (iii) the host has the capacity to remove that material and fails to do so within a reasonable period; (iv) having been put on notice of its defamatory character.[79] The defendant ('Demon') operated public newsgroup servers to which third parties could post messages that were stored automatically and made accessible to other newsgroup users for a fixed period. The case arose out of a 'squalid, obscene and defamatory' posting made by an anonymous user who impersonated the claimant (a practice known as 'frogery' or 'fraping').[80] Four days after being uploaded, the claimant notified the defendant of the posting and requested its removal. The defendant did not do so, and the post remained accessible until its scheduled expiry ten days later. The claimant only sought damages for publications occurring during this interval.

In the circumstances, Morland J concluded that the defendant's continued storage and transmission of the posting amounted to publication. The defendant was treated analogously to a traditional distributor, such as a bookseller or circulating library. Because it 'deliberately chose' to store postings and could 'obliterate' them at any time, Demon's conduct went beyond mere ownership of the storage equipment (which, by implication, would not be sufficient) and constituted *prima facie* publication — even without knowledge — since the material was defamatory 'on its face':[81]

> At common law liability for the publication of defamatory material was strict. There was still publication even if the publisher was ignorant of the defamatory material within the document. Once publication was established the publisher was guilty of publishing the libel unless he could establish ... that he was an innocent disseminator.[82]

Morland J appears to have understood cases like *Day v Bream* and *Emmens* as deciding that knowledge was relevant to innocent dissemination rather than publication. The Court adapted the 'proper inference' test from *Byrne*, suggesting a further analogy between an occupier's physical

---

[79] [2001] QB 201, 209, 212 (Morland J) ('*Godfrey*').

[80] 'Frogery' referred to the practice of impersonating a newsgroup user for the purpose of harming their online reputation. Today, 'frape' (a portmanteau of 'Facebook rape') is equivalent: see Rick Moen, 'Obfuscation Mitigation (Lexicon)' (11 December 2008) <http://linuxmafia.com/~rick/lexicon.html#frogery>.

[81] *Godfrey*, 203 (Morland J). See also Collins, above n 95 (ch 2), [15.06].

[82] *Godfrey*, 207 (Morland J).

control over premises and a web host's technical control over stored messages. However, this explanation could not justify liability before the point of notification, unless it takes the factually implausible view that the defendant has assumed a general responsibility for all stored messages. This approach also suffers from the basic problem that it treats publication as occurring without any positive act or authorisation by the putative publisher.

The distinction between messages defamatory 'on their face' and those whose meaning is less obvious is problematic in several respects. First, it is difficult to apply, requiring a host to read material and form a qualitative judgement about its meaning. This is both impracticable and ignores possible defences such as justification. Second, where statements are published by an automatic technical process, it is nonsensical to delimit publication liability by reference to a test that presumes human examination. Manual review would rarely (perhaps never) be required in other contexts, as *Day* and *Byrne* assumed. Finally, even if the distinction were workable, it would be inappropriate in an impersonation case such as *Godfrey*, where the statements *appeared* to originate from the claimant. Taken at face value, such statements could not be defamatory, since they would, on that assumption, have been consented to by their apparent author.[83] Such statements can, of course, be highly defamatory, despite appearances[84] — a conclusion at odds with the approach in *Godfrey*.

(b) *Subsequent decisions*

Later cases have tended to distinguish or confine *Godfrey*. For example, in *Tilley* Eady J interpreted *Godfrey* on the narrow basis that it was concerned with a single posting of which the host had specific knowledge, before going on to propose a test with a significantly higher threshold for ISPs.[85] Two other cases have directly addressed hosting liability, preferring an authorisation-based publication standard derived from *Byrne*.

In *Davison v Habeeb*, the fifth defendant ('Google') facilitated the publication and storage of defamatory articles on its Blogger.com hosted weblog service, an 'enormous burgeoning Babel' to which content is posted by its 400 million users at a rate of some 250,000 words per minute. Google did not create, select or approve Blogger content, but 'merely provides the tools for users

---

[83] In reality, the claimant also made 'puerile, unseemly and provocative' postings 'to tempt people to overstep the mark and defame the Plaintiff so that he can sue': *Godfrey v Demon Internet Ltd* [1999] (Unreported, High Court of Justice, Morland J, 23 April 1999), [14]–[16].

[84] See, eg, *Bryce v Barber* (Unreported, High Court of Justice, 26 July 2010) (awarding damages for 'Facebook rape').

[85] See below § 2.3.

to operate their sites'.[86] Google refused to delete the material without a court order on the basis that it did not know whether any of the allegations against the claimant were true.[87] Despite striking out the claim as an abuse of process,[88] HHJ Parkes QC reasoned that there was an arguable case that Google was a publisher of the material — at least after being notified by the claimant — because 'at some point' following notification it must be regarded as having consented to or acquiesced in publication, by analogy with the club operator in *Byrne*.

Like *Godfrey*, *Davison* fails to clarify whether publication requires actual knowledge. Notice was 'of cardinal importance', presumably reflecting the mental elements recognised in *Emmens* and *Byrne*,[89] but the precise moment of publication remains unclear. It is suggested that the approach should be the same as for website operators: until the point of notice, Google was an innocent disseminator, since it had exercised reasonable care despite being ignorant of the defamatory posting. After sufficient notice was given, it would no longer be an innocent disseminator, but due to its passivity nor would it necessarily be a publisher. The question is then whether Google can be inferred to have authorised or acquiesced in the publication, or otherwise by its conduct assumed responsibility for the words used; in almost all circumstances, the answer is likely to be 'no', but the possibility cannot be ruled out without considering the circumstances of publication and the intermediary's response in detail.

This was the approach preferred by the Court of Appeal in *Tamiz v Google Inc*, where the issue was whether Google was a publisher of defamatory comments posted to another Blogger weblog.[90] In that case, the Court rightly overturned the trial judge's conclusion that Google could *never* be a publisher, even after receiving notice and failing to act after a reasonable time. Applying *Byrne*, the essential issues were whether Google could 'be inferred to have associated itself with, or to have made itself responsible for, the continued presence of [the tortious] material on the blog'.[91] This would presumably involve considering how realistic such an inference was having regard to the scale of third party publications and the relationship between Google, bloggers and commenters. Although it seems doubtful whether such an inference is open on the facts of *Tamiz* (or indeed any case involving Blogger), these were essentially 'matters for argument' rather than

---

86 [2011] EWHC 3031 (QB), [17] (HHJ Parkes QC) ('*Davison*').

87 Ibid [11]–[15] (HHJ Parkes QC).

88 See below § 3.3(c).

89 *Davison*, [42] (HHJ Parkes QC).

90 [2012] EWHC 449 (QB), [38]–[39] (Eady J) ('*Tamiz*').

91 *Tamiz v Google Inc* [2013] EWCA Civ 68, [34] (Richards LJ) (Lord Dyson MR and Sullivan LJ agreeing) ('*Tamiz (CA)*'). The Court of Appeal otherwise upheld Eady J's approach as essentially sound: ibid [23].

summary judgment. This approach lacks the simplicity of a bright-line rule, but provides adequate certainty for intermediaries without conferring absolute immunity, which might retard genuine efforts to remove plainly tortious content.[92]

The comparison in *Davison* and *Tamiz* between Blogger and the notice-board in *Byrne* is open to two criticisms. First, unlike the defendant in *Byrne*, Google disclaims any personal endorsement of users' statements. HHJ Parkes QC concluded that Google 'appears to assume a degree of responsibility' for content on the basis of prohibiting various classes of material in its Blogger Contents Policy. However, there is no necessary inconsistency between reserving the contractual *right* to remove offensive or unlawful content, and the refusal to assume a *duty* to remove tortious material. In any case, the policy expressly preserves Google's right not to take action for violations,[93] and users promise to bear sole responsibility for their content.[94] Unless Google takes some specific action to approve or promote a specific posting, it is therefore difficult to see how merely operating the platform can be regarded as an assumption of responsibility for users' statements generally.

Second, Google possesses no practicable means to investigate each complaint, determine the applicable law, and verify the accuracy and lawfulness of posted material. Google's notice board is 'almost infinitely huge': if all Blogger postings were printed and pinned to an imaginary wall, its length would stretch three times around the earth and grow by roughly the distance from London to Oxford each day, weighed down by the postings of millions.[95] Even HHJ Parkes QC conceded that it is 'unrealistic' to expect removal of all material alleged to be defamatory. Unlike the clubhouse board in *Byrne*, it is unlikely that Google ever consents to any particular posting, tortious or not. Simply to acquiesce to all complaints would make 'significant inroads into freedom of expression', since not all allegations are well-founded.[96] Yet that is exactly what *Davison* appears to require, since — in the absence of a scalable way to determine whether content is tortious — hosts less well-resourced than Google will inevitably err on the side of caution. In *Tamiz*, Eady J accepted a less onerous metaphor, treating Google as the owner of a vast wall on which graffiti had been festooned overnight;[97] while it could paint or clean the wall, its failure to do so would not ordinarily entail consenting to the content of statements inscribed by the vandals.

---

92 The experience of absolute immunity in the United States is cautionary: cf *Communications Decency Act 1996* (US) 47 USC § 230; Lemley, above n 96 (ch 2), 112–13; Brian Leiter, 'Cleaning Cyber-Cesspools: Google and Free Speech' in Levmore and Nussbaum (eds), above n 85 (ch 1), 155, 172–3.

93 Google Inc, 'Blogger Content Policy' (2012) <http://blogger.com/content.g>.

94 Google Inc, 'Google Terms of Service (1 March 2012) <http://google.com/policies/terms/>.

95 This assumes that the average blog post comprises roughly one A4 page, stacked in columns of four sheets.

96 *Davison*, [45] (HHJ Parkes QC).

97 *Tamiz*, [10], [38] (Eady J).

The fact that Google also 'built' the wall and failed to install surveillance cameras was no more relevant than to the liability of the unfortunate property owner.

The Court of Appeal disagreed: because Google developed the platform and intended it to be used to post messages (unlike, presumably, the owner of a freshly-painted wall) on terms it specified, Blogger more closely resembled a notice-board than a defaced wall. The Court emphasised Google's volition in choosing to supply tools and operate a service for the dissemination of messages: in setting its terms and controlling its ultimate functionality, Google was more than a transmitting conduit, though not necessarily a participant.[98] Metaphor is apt to mislead. The debate about whether Blogger is 'like a notice-board' or 'like a graffiti wall' is ultimately less important than the assessment of its actual contribution to the publication in question. While it is true that Google's contribution goes beyond transmission to include storage of the defamatory words, the reality is that it still supplies, at most, an automated medium for storage and transmission. Its outward relationship to material does not change after notification, except to remove it. It remains essentially passive — indeed, it is normally this passivity, characterised by a failure to act at all, about which claimants complain. As Eady J remarked in *Tamiz*:

> It is not easy to see that [Google's] role, if confined to that of a provider or facilitator before [receiving notice], should be automatically expanded thereafter into that of a person who authorises or acquiesces in publication. … It takes no position on the appropriateness of publication one way or the other.[99]

On this view, a necessary but insufficient condition of publication is that the intermediary plays an 'active' role in approving publication. A neutral and passive role, in which the words are conveyed without human intervention, will be insufficient regardless of notice. This is consistent with the principle that a defendant is not liable in tort for involuntary or unintended actions.[100] The Court of Appeal seems to endorse this approach in *Tamiz*, with the qualification that a platform might eventually cease being 'purely passive' at least a reasonable period after notification.[101] Similarly, acquiescence might be inferred from ignoring a valid court order holding that the user's words are actionable.

Coherence and consistency in this emerging area of law demand that like services are treated alike. *Godfrey* is an outlier that predated the policies of protecting and balancing rights

---

98 *Tamiz (CA)*, [18], [24], [33]–[35] (Richards LJ).

99 *Tamiz*, [38] (Eady J).

100 *National Coal Board v J E Evans & Co (Cardiff) Ltd* [1951] 2 KB 861, 874–5 (Cohen LJ).

101 In *Tamiz*, five weeks elapsed from notification to removal, which was 'somewhat dilatory' and left room for such an inference: *Tamiz (CA)*, [35] (Richards LJ). It is illustrative of the difficulties involved that Google Inc received effective notice only when the claim form was issued: ibid [10].

expressed by Parliament in the *HRA*, and there are good arguments that it has already been abandoned. With the decision in *Tamiz (CA)*, a pattern appears to be emerging which treats platform operators and hosts as non-publishers until notification and, if the inference of acquiescence is open, *prima facie* publishers from a reasonable period thereafter. The basis for that inference is far from satisfactory, and the distinction between 'passive' and participatory hosts remains mired in confusion and metaphor. While it would be a matter for evidence, it is suggested that such an inference would rarely arise for automated services such as Blogger, which few would regard as consenting to words published by their users. To the extent they assumed otherwise, both *Davison* and *Tamiz* are at odds with the conclusion in *Tilley* that an ISP, there described as 'closely analogous' to Blogger,[102] is never a publisher. They are also inconsistent with treating search engines as non-publishers because they are 'entirely automatic' services that do not rely on human intervention.[103] Fortunately, the true *ratio* of *Davison* rests on abuse of process, while *Tamiz (CA)* recognised no more than the possibility of inferring acquiescence in an appropriate case, based on the traditional *Byrne* criteria.

2.3 ISPs

Although *Godfrey* is sometimes improperly described as an authority on ISP liability,[104] it is important to recall that that case concerned material uploaded to the defendant's newsgroup servers and stored in a persistent forum under its operational control, whereas an ISP provides transient routing facilities to access material stored by others.[105] The ephemeral nature of this role means that intermediaries who merely provide network connectivity will not, without more, be liable as publishers of defamatory material transmitted at the request of their subscribers.

Bunt v Tilley is the most recent authority on ISP liability.[106] Relevantly, the claimant alleged that three English ISPs had published defamatory newsgroup postings by transmitting them to message boards hosted by third parties. Eady J granted an application to strike out the claims

---

[102] *Tamiz*, [39] (Eady J).

[103] See below § 2.4. It is not easy to see why Google's choice to supply the Blogger service should lead to potential liability as a publisher of blog postings, but not its choice to offer a search service which lists defamatory results.

[104] See, eg, *Loutchansky v Times Newspapers Ltd [Nos 4 and 5]* [2002] QB 783, 813 (Lord Phillips MR); James Tumbridge, 'Defamation — The Dilemma for Bloggers and Their Commenters' [2009] *European Intellectual Property Review* 505, 506.

[105] The likely reason for *Godfrey* being misclassified as a case about ISP liability is that the defendant carried on business simultaneously as a provider of internet access and website hosting services. However, it was in its capacity as a website host and not an ISP that Demon published the defamatory statements.

[106] [2007] 1 WLR 1243 ('*Tilley*').

against the ISPs, concluding that they were not publishers of the defamatory material. Instead, they supplied a passive medium of communication without assuming any general responsibility for subscribers' statements. Eady J's approach to publication was to identify the specific causal contribution of each defendant: 'to focus on what the person did, or failed to do, in the chain of communication'.[107] Unlike Morland J in *Godfrey*, Eady J considered that publication entails a strong mental element, consisting of 'knowing involvement' in the relevant words:

> it is essential to demonstrate a degree of awareness or at least an assumption of general responsibility, such as has long been recognised in the context of editorial responsibility. ... [T]here must be knowing involvement in the process of publication of *the relevant words*. It is not enough that a person merely plays a passive instrumental role in the process.[108]

This partly explains why editors and commercial publishers are presumed from their position to intend to publish such libels, as Lord Morris reasoned in *McLeod*: they assume responsibility for the words that are published.[109] Similarly, it might reconcile the strict liability of printers and fault-based dissemination liability recognised in *Emmens* and *Vizetelly*: the latter are only 'knowingly involved' in publication where they knew or ought to have known of the defamatory words. By contrast, an intermediary which supplies a 'passive medium of communication' is not a publisher, since it does not assume any responsibility for the messages and has no knowledge of their contents. It is, in short, no distributor of the messages at all.

It follows that transmitting ISPs — and other network-layer conduits — can rarely if ever be described as publishers. While expressing caution about using imperfect analogies to describe new technical phenomena, Eady J accepted Collins' suggestion that such intermediaries are analogous to postal services and telephone carriers,[110] providing 'a means of transmitting communications without in any way participating in that process.'[111] On the facts, there was no evidence that any ISP had received proper notice from the claimant or 'sanctioned any publication with knowledge', even though only one ISP suspended the subscriber's connection upon learning of the proceedings. Accordingly, no defendant had participated 'in any meaningful sense' in publication.

Although this approach recognises the important technical distinctions between hosts and mere conduits, to rely on the criterion of 'knowing involvement' is problematic. First, publication

---

[107] Ibid 1249 (Eady J).

[108] Ibid [21]–[23] (Eady J) (emphasis in original).

[109] [1899] AC 549, 562 (Lord Morris) (noting that '[a] printer and publisher intends to publish, and so intending cannot plead as a justification that he did not know the contents').

[110] See Collins, above n 95 (ch 2), [15.38], [15.43].

[111] *Tilley*, 1246 (Eady J).

is concerned with the defendant's causal contribution to a communication of defamatory words *through its conduct*; its attitude towards the words being conveyed can have no bearing on whether or not that conduct has effected a publication, though it may supply an excuse for publishing as an innocent disseminator. Using knowledge to distinguish 'passive' from 'active' participants is, at best, unhelpful, because both ultimately contribute equally to the diffusion of tortious material. If, as Eady J suggested, prior awareness of defamatory material is what elevates involvement into 'knowing involvement', this test adds nothing. If the intermediary's contribution depends on its mental state, this risks distorting both concepts.

Second, *Tilley* fails to clarify the threshold of knowing participation. While it seems uncontroversial that granting permission is sufficient while innocent transmission is not,[112] the precise point at which an ISP will move from passive medium to active participant remains undefined. Because transmission is transitory, merely informing an ISP of a notorious subscriber's propensity to post defamatory material would not necessarily be enough to make it participate in subsequent publications, which are distinct. Further, the relationship between 'knowing involvement' and joint tortfeasance is unclear. It remains an open question whether an ISP could be liable for authorising or procuring a publication without 'knowingly participating' in it. Equally unclear is what action must be taken by an ISP who has been notified of defamatory material; disconnection of the user would usually be a disproportionate response, but the ISP would have no power to remove material which is hosted elsewhere. At best, it could block access to its other subscribers, a possibility discussed below in chapter 7. This issue did not arise in *Tilley* because none of the ISP defendants had received proper notice.

Finally, if participation requires acts which are directed to taking responsibility for the communication of specific words, this has the consequence that no liability can attach if it is impossible to read the defamatory statement. For example, if the words are encrypted, in a foreign language or otherwise obfuscated, an ISP cannot be 'knowingly' involved in their transmission. This is the problem of words not being 'defamatory on their face' in a different guise. The approach in *Tilley* represents a significantly higher threshold of publication than was recognised in *Godfrey*, and sets clear fault-based limits on the liability of secondary publishers. However, its analogy with postal services is unhelpful because their immunity derives from specific statutory provisions rather than general principles of publication. A better analogy is with the porter in *Day v Bream*, who was exonerated for innocently delivering sealed packages in the ordinary course

---

[112] *Tilley*, [21] (Eady J).

of business. Sealed packages have a more natural counterpart in the data packets delivered by ISPs.

2.4 Gateways

Like other application-layer services, search engines which actively participate in a publication can be liable as publishers, but not those which merely facilitate it. In *DesignTechnica*, the claimant (in addition to suing the website operator) alleged that Google was a publisher of defamatory 'snippets' which appeared in the third and fourth search results for the claimant. Google refused to remove the offending material from its search index. Google argued that it was, at most, a 'mere facilitator' of the defamation, since it had no control over the words displayed — which were selected automatically[113] — and could influence neither the keywords entered by its users nor the results they chose to access. Alternatively, Google relied on the statutory defence of innocent dissemination and safe harbours.[114]

Eady J held that Google was not a publisher of the search snippets.[115] Following *Tilley*, the test is 'whether the relevant Internet intermediary was *knowingly* involved in the publication of *the relevant words*'.[116] Prior to notification, Google lacked knowledge of the words appearing in the snippets; thereafter, Google had not authorised, approved or acquiesced in their publication simply by failing to remove them. The decisive factor was the lack of 'human input' by Google into its indexing and search functions, which were carried out by a web-crawling 'robot' rather than the conscious deliberations of human agents.[117] Their display was automatically triggered by the public's search queries rather than Google — a fact Eady J thought was 'fundamentally important'.[118] This automated quality and the large scale of Google's operations meant that no authorisation or intent to publish could be presumed from a failure to exclude a particular snippet from the index, even though it had actual knowledge.[119] Google therefore stood in a different position to a library whose cataloguer extracted defamatory snippets from a book. There the library must specifically select the material for inclusion and the words to be used, and can

---

[113] See Stephen Spencer, 'Anatomy of a Google Snippet' (18 March 2010) *Search Engine Land* <http://searchengineland.com/anatomy-of-a-google-snippet-38357>.

[114] See below § 3.1.

[115] *DesignTechnica*, [124] (Eady J).

[116] Ibid [36] (Eady J) (emphasis in original) (citing *Tilley*, [23]).

[117] *DesignTechnica*, [11]–[13], [53] (Eady J).

[118] Ibid, [50]–[51] (Eady J). Although Google now supplies suggested search queries, it is submitted that the same result would follow, since the suggestions are equally automatic.

[119] Ibid [51], [55], [57]–[58] (Eady J).

therefore be liable under the repetition rule. Google was simply a passive medium of communication, like the ISP in *Tilley*. Presumably, the same logic would apply where the defamatory matter is contained in a URL rather than a snippet.[120]

DesignTechnica reflects the general principle that, to be publishers, secondary disseminators must satisfy a mental element.[121] Failure to act after acquiring knowledge may support an inference that the search engine authorised, approved or acquiesced in the publication, but it must be possible and reasonable to remove the offending material.[122] Google could not prevent a particular snippet from appearing in search results — which might respond to similar queries or reference mirrored copies of material — without disproportionately affecting other search results. Another operative factor may have been the relative ease of including a '`robots.txt`' file on the DesignTechnica website, which could simply instruct Google's crawler (and those of other search engines) not to index the contents of that website.[123] The difficulty of removing the defamatory content took the facts outside *Byrne*, where removal was as simple as removing a sheet of paper. Hosts are not like search engines.[124] However, *DesignTechnica* leaves open the possibility that a search engine which can easily remove material may become a publisher after failing to do so within a reasonable time.

2.5 Preliminary conclusions

Several propositions may be derived from this brief survey of defamation claims against internet intermediaries. First, the scope of publication is becoming narrower. Where early authorities tended to impose *prima facie* liability, more recent authorities offer limited or total immunity. Application-layer platforms are unlikely to be publishers if they play a merely passive or instrumental role in conveying the defamatory words. Similarly, network-layer intermediaries who do no more than transmit, index or aggregate material without knowledge will not be publishers, provided that they take no position on the appropriateness of content, and act neutrally and passively. Only if the intermediary intervenes to promote or edit content, or *unreasonably* fails to act, could this amount to publication by authorising, approving or acquiescing in the words

---

[120] It is possible that the URL of a hyperlink might contain sufficient words to convey the false imputation, as in the case of a link which read 'http://www.dailynews.com/tech/2013/company-x-directors-490m-fraud-luxury-chalet-embezzlement.html'.

[121] *Emmens*, 357 (Lord Esher MR); *DesignTechnica*, [64]–[65] (Eady J).

[122] *DesignTechnica*, [49]; citing *Tilley*, [21].

[123] Ibid [58] (Eady J).

[124] Ibid [55] (Eady J).

used. This fault element means even actual knowledge will usually be insufficient if the defendant is a passive, neutral and automated medium of communication, subject to secondary liability as an authoriser.[125]

Although 'straightforward common law principles' of publication have been adapted to conduct by internet intermediaries,[126] it remains difficult to articulate a clear criterion to explain when a secondary party 'takes part' in publishing defamatory material, as distinct from merely facilitating or passively conveying it. The tendency to adopt different metaphors in similar cases has produced irreconcilable results and unpredictability in the principles applied (see Table 3). Despite this confusion, the commonality appears to be that non-publisher intermediaries neither assume responsibility for the defamatory words nor authorise their communication. Authorisation may be inferred from the combination of knowledge, control and inaction in limited circumstances, while assumption of responsibility may be inferred from conduct suggesting editorial control or proprietorship.

Case	Defendant	Test	Metaphor	Publisher?
Godfrey	Host of Usenet	*Prima facie* liability subject to *Emmens*	Owner of noticeboard	Yes
Tilley	Retail ISPs	Knowing involvement; not mere passive role	Postal service or telephone company	No
DesignTechnica	Search engine	Human input; not passive medium	Library catalogue distinguished	No
Kaschke	Website operator	Capacity to monitor or edit	N/A	Yes
Davison	Host of Blogger	Authorised or acquiesced in publication	Owner of noticeboard	Yes
Tamiz			Owner of graffiti wall	Possibly

Table 3: Outcomes in publication cases

Second, these common law limits upon the scope of publication, together with the statutory limitations considered below, act as strong deterrents of claims against intermediaries who host, cache or transmit defamatory material. This may partly account for the paucity of such claims, along with their disproportionate expense when compared to the damage suffered by the claimant. Section 4.3 identifies several more effective remedies.

---

[125] Cf Collins, above n 95 (ch 2), [15.42].

[126] *DesignTechnica*, [113] (Eady J).

Third, English courts exhibit reluctance to engage with policy arguments which favour limits on intermediary liability. This reflects an approach that regards internet publication as a matter to be fitted within the existing doctrinal framework, rather than as one element of a larger problem of internet content regulation. With few exceptions, courts have not considered whether remedies against secondary publishers would interfere with users' and intermediaries' fundamental rights.[127] However, even *prima facie* liability can encourage pre-emptive removal by intermediaries irrespective of the merits of an allegation and lead to conservative platform content policies which deter controversial speech. Given that almost all takedown requests never proceed to trial, this effectively lowers claimants' burden of proof in circumstances where intermediaries almost always lack the evidence necessary to plead a substantive defence. Anticipated liability also discourages investment in automated content analysis and moderation tools. Although recent limits on publication are welcome developments, the courts' failure to address these arguments largely ignores the important communications policies which underlie limits on secondary publishers' liability at common law.

3 Limitations upon secondary liability

To regard an intermediary as a non-publisher may be thought of as an *upstream* limitation on liability, in that it defeats any claim at a preliminary stage without having to raise a positive defence or contest the meaning and imputations of a statement.[128] Even if an intermediary is responsible as a publisher, several *downstream* limitations exist which carry over the policy of protecting innocent conduits from liability for tortious statements made by others: first, innocent dissemination within the meaning of s 1 of the *Defamation Act 1996* (UK) ('*1996 Act*'); second, the statutory safe harbours available under regulations 17–20 of the *E-Commerce Regulations*; and third, the defences of voluntary disclosure and non-primary publication proposed in the Defamation Bill 2012 (UK) ('2012 Bill'). Unlike pleas of justification or fair comment, which rely on external characteristics of the statement itself, these defences protect intermediaries based on their identity, mental state and relationship to the primary wrongdoer. This section argues that these defences support the legitimate policy of encouraging claimants to exhaust their remedies against primary wrongdoers, but criticises their imprecision, fragmentation, and failure to address more fundamental concerns over cost and procedure in defamation actions.

---

[127] Cf *DesignTechnica*, [42], [44] (Eady J).

[128] By analogy with Ronald Dworkin, 'Foreword' in Ivan Hare and James Weinstein (eds), *Extreme Speech and Democracy* (2009) 5, 8.

3.1 Innocent dissemination

Section 1(1) of the *1996 Act* provides that:

> In defamation proceedings a person has a defence if he shows that —
>
> (a) he was not the author, editor or publisher of the statement complained of,
>
> (b) he took reasonable care in relation to its publication; and
>
> (c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

The impetus for statutory reform emerged from concerns that the common law defence, which the Act 'superseded' (but did not expressly abolish),[129] was inadequate to protect intermediaries.[130] Section 1 was intended to modernise and expand the common law defence,[131] but its three conjunctive requirements offer narrower protection to internet intermediaries, since notice of allegedly defamatory matter is usually sufficient to defeat it.

(a) *Not the author, editor or publisher*

The first requirement excludes any defendant who played a part in composing the words complained of, such as their authors or editors, and any 'commercial publisher' whose business is to issue material to the public or a section of it.[132] In *DesignTechnica*, Eady J stated in *obiter* that this prevents commercial website operators from relying on the defence, since their businesses involve 'issuing material to the public'.[133] Such an approach would have the unintended effect of excluding any intermediary who disseminates a defamatory statement in the course of an information business. By contrast, *Godfrey* concluded that the defendants 'incontrovertibly can avail themselves of section 1(1)(a)', despite the fact that the ISP was in the business of storing and providing access to Usenet materials to a section of the public; namely, its subscribers. *Amazon* held that the defence applied where the website did not 'originate' material and merely supplied the system or service through which publication occurred.[134] To similar effect, *Tamiz* would have

---

[129] *DesignTechnica*, [70] (Eady J).

[130] Lord Mackay, *Reforming Defamation Law and Procedure: Consultation of Draft Bill* (July 1995) [2.5], [2.6].

[131] Cf New South Wales Law Reform Commission, *Report 75 — Defamation* (1995) [9.9] <http://www.lawlink.nsw.gov.au/lrc.nsf/pages/R75CHP9> (concluding that reform is better left to the courts, since legislative intervention could 'stultify the development of the law').

[132] See *1996 Act* ss 1(2), 17(1) ('publisher' not to be given its common law meaning).

[133] *DesignTechnica*, [80] (Eady J).

[134] *Amazon*, [40]–[41] (HHJ Moloney QC).

treated Google as outside the definition of 'commercial publisher', because material was issued to the public by Blogger's *users* and not Google itself.

This view of paragraph (1)(a) is clearly more consistent with the text and purpose of s 1, which was intended to apply to new media[135] and protect 'a conduit which has enabled another person to publish defamatory material'.[136] It is also subservient to subsection (3), which gives non-exhaustive examples of activities deemed innocent dissemination; among them are 'providing any ... service by means of which the statement is ... made available in electronic form'[137] and 'provid[ing] access to a communications system' without 'effective control' over its users. Only if the intermediary goes beyond these activities — for example, by composing, selecting[138] or editing material — might it fail to satisfy the condition. The contrary view would render s 1 completely ineffective at protecting providers of commercial internet services.

(b) *Reasonable care in relation to publication*

Second, secondary publishers must exercise due care in relation to a publication. This involves considering the extent of their responsibility for the statement, the nature or circumstances of its publication, and any previous conduct or character of the primary wrongdoer.[139] Although there is little case law interpreting this duty, it appears difficult to satisfy where the secondary publisher acts passively. In *DesignTechnica*, Eady J found it 'difficult to comprehend' how Google could satisfy paragraph (1)(b) when publication occurred automatically without human input.[140] HHJ Moloney QC refused to strike out the claim in *Amazon* for this reason, though noted the possible counter-argument that pre-moderation was not reasonable on a 'vast website'.[141] Conversely, in *Tamiz* Eady J thought it not 'outside the bounds of a reasonable response' for Google not to investigate content published on Blogger — because there it did pass complaints to the primary author.[142] In *Tilley* the ISPs' contractual terms, which prohibited subscribers from publishing defamatory statements, were evidence of reasonable steps, though they took no steps to enforce them.[143] Given that Google's policies also prohibit defamatory content, *Tilley* and

---

[135] Mackay, above n 130, [2.3].

[136] Hansard, Defamation Bill, House of Lords (2 April 1996, Lord Chancellor) col 214.

[137] *1996 Act* s 1(3)(c).

[138] An example might be readers' comments in a newspaper (whether published in print or online).

[139] *1996 Act* s 1(5).

[140] *DesignTechnica*, [74] (Eady J).

[141] *Amazon*, [44] (HHJ Moloney QC).

[142] *Tamiz*, [47] (Eady J); aff'd *Tamiz (CA)*, [42]–[43] ('a generous view' but not wrong).

[143] *Tilley*, [63]–[66] (Eady J).

DesignTechnica are difficult to reconcile. Ultimately, once an intermediary is given notice, failing to act is 'an insuperable difficulty' to establishing reasonable care[144] — a view supported by extrinsic materials.[145]

(c) *No actual knowledge or wilful blindness*

Third, the secondary publisher must not know or have reason to believe that its conduct contributes to the publication of the defamatory statement. These words 'import the concept of recklessness'[146] rather than constructive knowledge; they operate on what the defendant actually knew. However, a good faith belief that a defamatory statement is justified (for example, because true or privileged) will not satisfy paragraph (1)(c).[147] The defendant must be an 'unwitting contributor' to publication and have 'no idea of the defamatory nature' of material.[148] Thus, in *Godfrey* and *Tamiz*, the defence was unavailable once the defendant had been notified. At that point, even with an assurance of truth from the author, the intermediary would have cause to believe that its services were contributing to a relevant publication.[149] However, in *Tilley*, two of the defendant ISPs were held to satisfy paragraph (1)(c) because they never received proper notice.[150] The combined effect of paragraphs (a)–(c) is to exclude reliance upon the statutory defence after an intermediary receives valid notice from the claimant. This means that it adds little to the common law protections for secondary disseminators considered above.

3.2 Safe harbours

As discussed in chapter 3,[151] intermediaries that qualify as information society service providers are protected from certain defamation liability by the *E-Commerce Regulations*. This section argues that, of the three safe harbour activities, mere conduit and caching are unlikely to provide protection beyond the common law. Storage is the most important safe harbour, but its limits are unclear and defined by reference to knowledge, which perversely discourages voluntary content

---

144 *Godfrey*, 206 (Morland J).

145 Mackay, above n 130, [2.4].

146 *Milne v Express Newspapers* [2005] 1 WLR 772, 788 (May LJ) (in the context of s 4(3)).

147 Hansard, Defamation Bill, House of Lords (2 April 1996, Lord Williams) col 216.

148 Hansard, Defamation Bill, House of Lords (2 April 1996, Lord Mackay LC) col 214.

149 *Tamiz (CA)*, [44]–[46] (Richards LJ).

150 *Tilley*, 1261 (Eady J).

151 See above chapter 3, § 2.1.

moderation while rewarding reflexive removal. Despite this, the safe harbours have generally shielded intermediaries from monetary liability in defamation claims (see Table 4).

Case	Defendant	Publisher?	Mere conduit?	Storage / caching?	Result
Godfrey	Host of Usenet	Yes	N/A — prior to *Regulations*		Liable
Tilley	Retail ISPs	No	N/A (Yes)	N/A (Yes)	Not liable
DesignTechnica	Search engine	No	No	No	Not liable
Kaschke	Website operator	Yes	No	Yes	Not liable
Davison	Host of Blogger	Yes	No	Yes	Not liable
Tamiz		Possibly	No	Yes (at trial)	Not liable

Table 4: English defamation cases involving safe harbours

(a) *Mere conduits*

An intermediary's mental state is immaterial to regulation 17, which therefore affords considerably broader protection than s 1 of the *1996 Act*. Despite this, there are few examples of its application. *Tilley* appeared to treat the safe harbour as applicable to retail ISPs, but it was unnecessary to reach a conclusion.[152] In *DesignTechnica*, Eady J remarked that (unlike other member states) Parliament had chosen not to extend conduit protection to search indices,[153] which are permanently stored.[154] However, because it is the *display* of results, rather than the antecedent generation of an index, that might constitute publication, this could be sufficient for gateway immunity in respect of transmission.

(b) *Caching*

Regulation 18 has a broader operation than s 1 of the *1996 Act*, since a defendant who has been put on notice of defamatory material could not satisfy s 1(1)(c), but may still attract caching protection until a reasonable period after acquiring knowledge that the source material was removed or made subject to a removal order. In *Tilley*, Eady J accepted evidence that an ISP's

---

[152] See *Tilley*, 1254–5, 1260 (Eady J).

[153] Department of Trade and Industry, *Consultation Paper on the Electronic Commerce Directive* (June 2005) [4.2]–[4.7] <http://www.bis.gov.uk/files/file13986.pdf>.

[154] *DesignTechnica*, [89] (Eady J).

proxy web cache would satisfy the requirements of regulation 18 where it temporarily stored defamatory newsgroup materials.[155]

(c) *Hosting*

Regulation 19 is the most important safe harbour in defamation claims. The scope of protection is broader than under the *1996 Act* in two respects. First, the object of knowledge is higher — unlawful rather than merely defamatory material — and, second, immunity continues until a reasonable interval after notification. Because unlawfulness requires the defamatory statement to be actionable, which is to say, made in the absence of justification or another defence, regulation 19 appears to require knowledge of both a statement and the facts or circumstances which render it (or its imputations) false or malicious.[156] However, if defendants go beyond mere storage of information to select, modify or generate the impugned materials, they will lose safe harbour protection. These two issues are discussed below.

(i) *Knowledge of unlawfulness*

The knowledge required is of a statement's *actionability* rather than its defamatory character.[157] Unless a notice provides sufficient information from which the unlawfulness of the words could be ascertained (for example, falsity), the defendant will lack knowledge; in effect, this acts as a double-reversal of the onus of proof. In *Karim v Newsquest Media Group Ltd* the Court granted summary dismissal where the defendant ('Newsquest') had stored defamatory comments alongside an article reporting on the claimant solicitor's disciplinary proceedings.[158] Before notification, Newsquest did not have actual knowledge; thereafter, it expeditiously removed the articles and their associated comments. The main difficulty with this outcome is that the article was held to be protected by qualified privilege, yet pre-emptively removed (along with public debate) to preserve safe harbour protection. This suggests that regulation 19 does little to remove the incentive for over-compliance faced by intermediaries who are unable (or unmotivated) to plead substantive defences.

Short of granting absolute immunity, this incentive cannot be completely removed. However, it can be minimised by adopting a default position which absolves intermediaries from the onerous task of passing judgment on impugned materials. The prevailing approach is to

---

[155] *Tilley*, [52]–[53] (Eady J).

[156] See Collins, above n 95 (ch 2), [17.25].

[157] *Kaschke*, [100]–[102] (Stadlen J).

[158] [2009] EWHC 3205 (QB), [15] (Eady J) ('*Newsquest*').

require, as part of giving valid notice, sufficient details of why a statement is unlawful. In *Amazon*, the claimant failed to specify the specific book reviews and comments about which he complained, which made it impossible for Amazon to perform the 'exercise of discrimination' required to separate legitimate criticism from defamatory statements. The claimant also failed to explain why each posting was unlawful, so that Amazon could not 'investigate or adjudicate upon it'.[159] This reflects a proper understanding of the way in which regulation 19 shifts the burden onto complainants to justify their allegations. Adopting a higher threshold of actual knowledge reduces the risk of wrongful removal without prejudicing genuine claims.

In *Davison*, HHJ Parkes QC applied *Tilley* and *Kaschke* to conclude that a platform must know sufficient facts to assess the strength of available defences. Without information one way or the other, it could not be aware of facts from which unlawfulness would have been apparent.[160] This is consistent with the approach taken in *eBay (CJEU)* that protection is only displaced by knowledge of facts or circumstances from which 'a diligent economic operator should have identified the *illegality* in question'.[161] For such knowledge to arise, a notice must not be 'insufficiently precise or inadequately substantiated'.[162] In *Davison*, Google received correspondence from both claimant and primary author in which each attempted to substantiate their allegations against the other; faced with two irreconcilable notices, it had 'no possible means one way or the other to form a view as to where the truth lies.'[163] In those circumstances, Google could not be said to meet the threshold of knowledge required to divest it of immunity.

Davison suggests that an intermediary will be able to rely on the storage safe harbour notwithstanding its receipt of notice from the claimant in three circumstances. First, if the notice is invalid, in the sense of being imprecise or unsubstantiated, it will not be effective to confer actual knowledge or awareness. Second, if the notice makes allegations of unlawfulness, which are disputed by the primary author on some credible basis, then unlawfulness could not be inferred. In effect, disputation would operate analogously to a counter-notification.[164] Third, if the claimant gives notice, but the intermediary otherwise becomes aware of facts suggesting that the material is justified or privileged, or that the claim would fail, then the intermediary will not have knowledge of unlawfulness. These circumstances sensibly reflect the fact that an intermediary is

---

[159] *Amazon*, [47]–[48] (HHJ Moloney QC).

[160] *Davison*, [63] (HHJ Parkes QC). Cf Brian Neill and Richard Rampton (eds), *Duncan & Neill on Defamation* (2nd ed, 1983) [20.20].

[161] *eBay (CJEU)*, [120] (emphasis added).

[162] Ibid [122].

[163] *Davison*, [66] (HHJ Parkes QC).

[164] Cf *DMCA* § 512(g).

normally 'in no position to adjudicate' a complex factual and legal dispute between prospective litigants.[165]

Tamiz provides another example of notices which failed to confer knowledge of actionability. Applying *eBay*, the trial judge held that notices alleging defamation — without giving any details of falsity or the inapplicability of obvious defences — were neither sufficiently precise nor substantiated that a diligent host should have identified the statements' unlawfulness. While it was 'implicit' in the complaints that Mr Tamiz denied the allegations of theft and drug dealing, Google was not required to accept complaints at 'face value' to retain protection.[166] This is clearly consistent with the *ratio legis* of regulation 19, which is designed to immunise hosts unless they have *actually* acquired reasonably sufficient evidence of unlawfulness.

(ii) *Conduct going beyond storage*

Voluntary content moderation which goes beyond storage activity is not protected. In *Kaschke*, Stadlen J doubted whether regulation 19 would apply to a defendant who 'on a few occasions' removed offensive or inappropriate postings from hosted weblogs. While it did not matter that the defendant supplied other non-storage services (such as self-published material), the 'particular information' in respect of which protection is sought must consist solely of storage.[167] This approach is clearly problematic for application-layer intermediaries who voluntarily moderate content and arguably frustrates the purpose of the Directive by discouraging efforts to remove harmful and offensive internet content.[168] Conversely, in *Newsquest* the Court concluded that regulation 19 applied even though the defendant had authored other, non-tortious content on the webpage concerned, and had the capability to moderate comments.[169]

For similar reasons, it is unlikely without statutory intervention that regulation 19 would protect *all* activities by Google and other search engines.[170] Although search engines are 'hosts' in respect of third parties' information automatically stored on their servers, peripheral data processing, advertising and curated content would normally involve selecting or modifying data in ways that precluded protection.

---

[165] Ibid [68] (HHJ Parkes QC).

[166] *Tamiz*, [59]–[60] (Eady J).

[167] *Kaschke*, [71]–[72], [74]–[75] (Stadlen J).

[168] Cf ibid [87]–[88] (Stadlen J).

[169] *Newsquest*, [15] (Eady J).

[170] *DesignTechnica*, [112] (Eady J).

3.3 Other limitations

Three recent developments further reduce the availability of monetary remedies against intermediaries.

(a) *Exhaustion of primary claims*

Clause 10 of the 2012 Bill would remove all jurisdiction to hear defamation actions against intermediaries who are not the author, editor or commercial publisher of the statement complained of, unless it is 'not reasonably practicable' to proceed against any of those primary parties. This applies to both offline intermediaries, such as booksellers, and all internet intermediaries.[171] If enacted, this provision would drastically curtail the responsibility of intermediaries, who would not face liability unless the claimant could first clear the threshold of proving impracticability. This proposal expresses a clear policy of encouraging complainants to resolve disputes directly with primary wrongdoers (and limited relational secondary wrongdoers, such as employers) rather than pursuing intermediaries. However, the proposal is incomplete and suffers from several defects.

First, the threshold of impracticability is unclear. If material is posted anonymously, a claimant might yet obtain voluntary disclosure — or, failing that, a *Norwich Pharmacal* order — from the intermediary and thereby proceed against the primary party. This would, presumably, be reasonably practicable; a lower threshold of practicability would deprive this limitation of its intended effect. Second, although clause 10 excludes any 'action for defamation', it is unclear whether it prohibits joinder of intermediaries for the purpose of injunctive relief — though joinder solely for that purpose may well be disproportionate if the claimant could already enjoin the primary author.[172] Third, because clause 10 does not displace the traditional rules on publication and safe-harbours, intermediaries may still need to remove content on the assumption that action against the primary tortfeasor may be unavailable. Despite these problems, clause 10 properly directs claimants' attention to primary wrongdoers before seeking to shift losses and enforcement costs onto secondary parties.

---

[171] Parliamentary Research Paper 12/30, Defamation Bill No 5 2012–13 (28 May 2012) 20.

[172] *Davison*, [69] (HHJ Parkes QC).

(b) *Voluntary disclosure*

The second defence introduced by the 2012 Bill protects website operators who were not the ones who 'posted' a defamatory statement. This defence applies unless it is not possible for the claimant to identify the person responsible and he 'gave the operator a notice of complaint' about the statement, to which the operator failed to respond as required by regulations.[173] Where material is posted with attribution, this confirms that the intermediary need do nothing: the claimant's grievance lies with the primary author. Where it is posted anonymously, website operators must voluntarily disclose the poster's identity to retain their immunity. Having done so, they then remain protected even after acquiring actual knowledge of actionable material.

As will be argued in chapter 6, identity disclosure is a vital part of any effective system of internet enforcement. The new defence of voluntary disclosure primarily benefits application-layer intermediaries who are considered publishers of user-created content, since existing case law exonerates many gateways, ISPs and hosts at the publication stage. However, clause 5 also creates several problems. First, like s 1 of the *1996 Act*, clause 5 may be less attractive to intermediaries than passive inactivity, since the claimant bears the onus of proving publication, while the defendant would have to raise and prove each element of the defence.[174] Second, 'website operator' is not defined by the bill. To limit the defence arbitrarily risks redundancy in an age of 'apps' and platforms, but this approach creates uncertainty. Further complications arise on weblog and cloud services, for which there may be multiple potential operators.

Third, unlike *Norwich Pharmacal* orders, clause 5 makes no provision for public interest anonymity. Voluntary disclosure should not lead to websites being encouraged to disclose the identity of people whose anonymity it is in the public interest to preserve. Widespread disclosure without judicial supervision would make it much harder for people to write anonymously about controversial but lawful topics, and may expose activists in developing countries to harm. Fourth, clause 5 is likely to encourage automatic disclosure by risk-averse website operators who fear the absence of the defence if they fail to comply. Unlike the judicially-mediated *Norwich Pharmacal* procedure, this invites opportunistic allegations of defamation to discover primary authors' identities cheaply; to give disclosure may invade their privacy if there is no arguable, let alone actionable, wrong.

---

[173] Defamation Bill 2012 (UK) cl 5.

[174] Graham Smith, 'What the Defamation Bill Means for the Internet' (17 May 2012) *Inforrm's Blog* <http://inforrm.wordpress.com/2012/05/17/what-the-defamation-bill-means-for-the-internet-graham-smith/>.

Fifth, the threshold of 'possible' identification is unclear. It suggests a higher standard than 'reasonably practicable', yet if the operator possesses the information (which clause 5 presupposes, since without it the operator could disclose nothing), then it will be 'possible' to obtain it via a *Norwich Pharmacal* application and clause 5 will have no application. Conversely, if judicial disclosure has been sought and failed, then voluntary disclosure is unlikely to be appropriate. Sixth, the degree of identification is unclear. An IP address might be all that the website operator possesses, so the claimant is still likely to need *Norwich Pharmacal* relief against, at a minimum, the tortfeasor's ISP.

Seventh, the Bill does not address the problem of 'casual threats of litigation'[175] being made against website operators in order to compel withdrawal of unsavoury but non-tortious material by people who wish to remain anonymous for other reasons.[176] The prospect of defending costly proceedings is at least as chilling when threats are made to primary authors rather than intermediaries, since authors are typically one-shot defendants who lack the specialist advice or resources necessary to defend claims. For this reason, clause 5 fails to solve the problem of intimidation, and risks being turned into a vehicle for reputation management. Disclosure and take-down may prove even more chilling than pure take-down, unless the cost of defending an unmeritorious action can be substantially reduced.

Eighth, the notice of complaint only has to specify why the statement is defamatory. This ignores possible defences available to the original poster, which might mean that the statement, although defamatory, is not actionable. Disclosure might therefore be given on the basis of true statements which involve no tort, which may lead to the surprising result that clause 5 does not apply but the website operator has a defence under the storage safe-harbour. Finally, clause 5 discourages content moderation by failing to protect a website operator who amends user-created content in good faith. Most of these issues could be avoided with appropriate guidance and limitations. Despite its many problems, clause 5 reflects the desirable policy of encouraging complainants to resolve disputes directly with primary wrongdoers, rather than pursuing monetary remedies against secondary publishers.

---

[175] Hansard, House of Commons, Defamation Bill 2012 (Second Reading, 12 June 2012, Mr Sadiq Kahn MP) col 193.

[176] Alastair Mullis and Andrew Scott, 'Missing the Wood (with no Excuses): The Defamation Bill 2012' (6 June 2012) <http://blogs.lse.ac.uk/mediapolicyproject/2012/06/06/missing-the-wood-with-no-excuses-the-defamation-bill-2012/>.

(c) *Abuse of process*

Abuse of process offers a basis for striking out actions against intermediaries where there has been no real or substantial tort. As the Court of Appeal held in *Jameel v Dow Jones & Co Inc*, defamation proceedings will be dismissed where there is no realistic prospect that they would yield any legitimate advantage that outweighs their cost and expense — in other words, where 'the game is not worth the candle'.[177] Although once rejected in *Goldsmith* as a question for Parliament,[178] this principle now follows from s 6 of the *HRA* and the overriding objective, which oblige courts to protect the rights of defendants in actions which are not necessary and proportionate to protecting the claimant's reputation.[179] For example, in *Kaschke*, proceedings were not proportionate because the original posting had been removed and a right of reply already published three years earlier; a claim against the website operator was therefore unlikely to vindicate the claimant any further.[180] In *Davison*, the claimant's action against Google was disproportionate considering the limited extent of publication, especially when she had remedies against the primary authors.[181] The same was true of the action in *Tamiz*, where — even though the comments were visible for a longer period — they had since 'receded into history' and caused minimal damage.[182] Accordingly, even if claims technically lie against intermediary distributors, it would not often be a proportionate use of the Court's resources or compatible with defendants' and users' rights to allow them to proceed.

4 Conclusion

This chapter has examined the development of liability rules in defamation actions against network and application-layer intermediaries. Their liability as publishers and joint tortfeasors has been progressively limited by two influences; first, judicial clarification of the scope of publication at common law; and second, *sui generis* defences and doctrines of proportionality. These limitations are heavily indebted to the liability rules developed in disputes involving offline intermediaries and previous generations of communications technology, reflecting their iterative

---

[177] [2005] QB 946, 966, 969–70 (Lord Phillips MR) ('*Jameel*').

[178] *Goldsmith*, 498 (Scarman LJ) (refusing to extend the traditional restriction on proceedings commenced for an ulterior purpose), 503 (Bridge LJ) (considering the proper limits a matter for Parliament).

[179] *Jameel*, 962 (Lord Phillips MR); *Hays*, [37], [61]. See also *Civil Procedure Rules* r 1.1.

[180] *Kaschke v Osler* [2010] EWHC 1075 (QB), [25], [31] (Eady J). See also *Hays*, [59]–[60] (Tugendhat J) (striking out claim against weblog operator).

[181] *Davison*, [27] (HHJ Parkes QC).

[182] *Tamiz (CA)*, [50]; *Tamiz*, [50].

and analogical nature as 'indicia of the law's capacity for growth and adaption'.[183] Modern courts continue to apply them, but place greater emphasis upon fault and the availability of statutory safe-harbours. The collective effect of these limitations is to resist the impetus for intermediaries to assume a role as 'content police' on the internet, absolving them from monetary liability if they fail pre-emptively to verify, monitor or remove defamatory material authored by others.

Section three identified several limitations and defences which protect intermediary–publishers from monetary liability. However, it is important not to deter *all* forms of enforcement by intermediaries. The basic challenge confronting policymakers is how to provide redress to claimants which is both effective and proportionate to the protection of their reputations without chilling non-tortious speech or discouraging innovation in online services. This section explains this tension before identifying several new injunctive remedies which complement existing limitations under traditional liability rules.

4.1 The need for effective remedies

The internet has dramatically increased the extent to which defamatory statements are communicated, consumed and remembered. First, it makes possible communications between individuals and other members of the public 'at virtually no cost',[184] which makes defamatory material more common and widespread. Second, because material is easily accessed and propagated, the 'poison tends to spread far more rapidly' online.[185] Third, its permanence is prolonged thanks to search engines, caches and archives.[186] Fourth, claimants may be disadvantaged in claims against intermediaries who are, through their online activities, 'repeat players' in defamation litigation.[187] Fifth, traditional remedies will often be futile where the defamatory words are published anonymously or from a place where intermediaries enjoy stronger protections. Jurisdictional competition for intermediaries' business and incompatible national speech values make this form of regulatory arbitrage inevitable.[188]

---

[183] R C Donnelly, 'History of Defamation' [1949] *Wisconsin Law Review* 99, 123, 124.

[184] *The Law Society v Kordowski* [2011] EWHC 3185 (QB), [180] (Tugendhat J).

[185] *Cairns v Modi*, [123] (Bean J). Cf *Ley v Hamilton* (1935) 153 LT 384, 386 (Lord Atkin) ('It is precisely because the "real" damage cannot be ascertained and established that the damages are at large. It is impossible to track the scandal, to know what quarters the poison may reach …').

[186] See, eg, Leiter, above n 92, 162.

[187] See generally Marc Galanter, 'Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change' (1974) 9 *Law & Society Review* 95.

[188] See, eg, see *Communications Decency Act 1996* (US) 47 USC § 230(c)(1); *United States Constitution*, amend I.

Although not all these factors are unique to the internet, the common law has always been concerned that new technologies which assist the spread of defamatory material should be brought within its control. As Brett J (who would later decide *Emmens*) cautioned in a decision recognising publication by telegraph:

> It was never meant by the legislature that these facilities for postal and telegraphic communication should be used for the purpose of more easily disseminating libels.[189]

Without meaningful ways to target offshore and anonymous internet material, it may be impossible for claimants to obtain redress — particularly if damages against the enabling intermediaries are excluded by the doctrines discussed in section 3. These factors make it imperative for courts to develop alternative responses to internet defamation.

4.2 Freedom of expression

In many cases, prompt removal of defamatory material offers satisfactory redress without the need for further litigation.[190] Indeed, the effectiveness of removal is one reason why the number of claims against intermediaries remains low despite self-evident growth in the quantity of defamatory internet publications. If a claimant seeks only a retraction or apology, proceedings against an intermediary offer few additional benefits — a fact acknowledged in *Davison* and *Kaschke* — but carry higher costs and potential for adverse publicity.[191] However, removal is imperfect: it may be unavailable from platforms and gateways that rely on primary authors to withdraw defamatory material (as in *Tamiz*); when it is available, removal tends to produce significant over-enforcement characterised by 'spill-over' removal of non-tortious content.

The relationship between removal and freedom of expression is complex. In *Reynolds v Times Newspapers Ltd*, Lord Hobhouse remarked: 'There is no human right to disseminate information that is not true.'[192] Although this statement must be qualified — certain untruths, such as satire, honest opinion and responsible journalism may be lawfully published — it reflects the obvious premise that removing material interferes with authors' and readers' freedom of expression only to the extent that non-tortious information is affected. Article 10(2) of the *Convention* acknowledges this by permitting derogations 'for the protection of the reputation or

---

189 *Williamson v Freer* (1874) LR 9 CP 393, 395 (Brett J).

190 See, eg, *Pepin v Taylor* [2002] EWCA Civ 1522 (claim involving libellous messages posted by the defendant on a public internet newsgroup).

191 Claimants also realise that litigation carries the potential to cause significant reputational harms of its own. See above chapter 1, § 2.3.

192 [2001] 2 AC 127, 238 (Lord Hobhouse).

the rights of others'. The relevant question is therefore to what extent secondary liability rules encourage the removal of non-tortious statements. This may occur in several ways.

First, despite *Tamiz*, the *prima facie* burden on claimants remains low — to notify the defendant (usually electronically) of defamatory material, giving details of its actionability. Intermediaries are not obliged to consider both sides of the argument, let alone conduct their own investigations into the merits of any possible defence, since this is costly and impracticable in large volumes. Second, even were they so inclined, intermediaries will almost never possess the evidence necessary to raise substantive defences to a defamation claim since they are not involved in the composition of defamatory material. This may prevent relevant limits on claimants' rights from being pleaded and cause non-tortious content to be removed.[193] Once an intermediary has been notified, removal is usually the most sensible course, since it may be unclear whether the notification confers sufficient knowledge to exclude protection. This risk is especially harmful to bloggers, whose reportage frequently serves valuable public interests.[194] Third, intermediaries typically wish to avoid a protracted dispute, since there may be substantial costs even if the claimant fails at trial. Even well-founded but disproportionate claims have the potential to interfere with freedom of expression.[195]

4.3 Alternatives to notice-and-takedown

The modern approach to publication by passive intermediaries solves these problems by effectively requiring claimants to prove their case at trial before an intermediary will come under a duty to remove content. While this recognises that the Court is usually in the best position to determine whether material is tortious, the cost of pursuing a defamation complaint to trial is prohibitive and may frustrate many legitimate claims. This section identifies three possible alternatives.

(a) *Disclose-and-indemnify*

Clause 5 of the 2012 Bill creates a defence of disclosure, which makes it easier for claimants to identify, contact and, if necessary, obtain injunctive relief against the primary authors of material. This approach protects freedom of expression without depriving claimants of a remedy; it solves

---

193 *Hays*, [66].

194 Ibid [61]. See, eg, Paul Staines and Harry Cole (eds), 'Guido Fawkes' Blog' (9 January 2004) <http://order-order.com/> (political commentary and gossip read, but often unpublished, by the mainstream press).

195 See above § 3.3(c).

a basic problem of high transaction costs between intermediaries and primary authors, allowing the latter to assume the risk that information is tortious and so make the decision whether to leave impugned materials online. While this approach is imperfect for the reasons noted previously, it reflects a fairer balance between the rights of authors, intermediaries and claimants. As proposed in chapter 8, the disclose-and-indemnify approach should arguably be extended to other torts.[196]

(b) *Alternative dispute resolution*

It is telling that defendants to defamation proceedings are often more afraid of the cost of winning than the likelihood of losing. A second set of solutions therefore focuses on reducing the cost of resolving defamation disputes. While a full examination of these proposals is beyond the scope of this research, their basic aim is to supply a mechanism by which the status of allegedly defamatory material can be quickly and cheaply determined. This could occur in two ways. First, a specialist tribunal, such as the Information Rights Tribunal,[197] could be vested with specific authority to hear internet content disputes below a threshold monetary value. Second, by analogy with the UDRP, a uniform dispute resolution process could be established, either under the auspices of ICANN or a national or regional regulator, under which claimants and intermediaries could submit to common principles for content disputes. Intermediaries who participated in the scheme might be granted conditional immunity from monetary liability, in return for taking any action required of them by the arbitrator. Courts could then enforce the pre-action protocol for defamation cases more strictly and refer appropriate matters for early neutral determination in accordance with the procedure for a fixed fee, while abuse of process can continue to be used to remove disproportionate claims from the court system.

(c) *Discursive remedies*

A third possibility is to require storage intermediaries to publish corrections or disputations without monetary liability and thereby avert much of the injury caused by defamation without harming freedom of expression. These amendments could only be published by the host or cache of material (because conduits could not easily detect and update it during transmission), but could occur with or without the primary author's cooperation. As Mullis and Scott have argued,[198]

---

196 See below chapter 8, § 2.5.

197 See *Tribunals, Courts and Enforcement Act 2007* (UK) s 3; *Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009* (UK) r 3(1).

198 See Andrew Scott, 'Reframing Libel: Taking (All) Rights Seriously and Where it Leads' (2012) 63 *Northern Ireland Legal Quarterly* 5; Andrew Scott and Alastair Mullis, 'The Swing of the Pendulum: Reputation, Expression and the Recentering of English Libel Law' (2012) 63 *Northern Ireland Legal Quarterly* 27.

defamation should recognise discursive remedies which give defamed claimants what they really want without the need for protracted and costly court procedures; namely, an opportunity to reply with their side of the story and to have the true facts published in place of (or alongside) the false ones. While a discursive response could not provide full vindication in all cases, it would offer a cheap, speedy way for claimants to correct or dispute the veracity of statements concerning them without interfering with freedom of expression, innovation or neutrality. Once a discursive remedy has been obtained, little purpose is served by a claim against an intermediary — except to enforce the discursive remedy itself. The availability of non-monetary injunctive relief is considered further in chapter 7.

5
Copyright

Copyright, it is said, is one of the great balancing acts of the law.[1] The rights it confers embody the basic tension between encouraging optimal creation and consumption of works; their boundaries reflect delicate compromises between creators, consumers, disseminators and many other interest groups. These conflicts are exemplified in the enforcement of copyright against internet intermediaries. Copyright owners assert that almost one quarter of global internet traffic,[2] 80 per cent of YouTube videos,[3] and 97 per cent of BitTorrent transmissions infringe their

---

1 Sam Ricketson, 'Copyright' in Blackshield, Coper and Williams (eds), *The Oxford Companion to the High Court of Australia* (2001) 152, 154.

2 David Price, 'Technical Report: An Estimate of Infringing Use of the Internet – Summary' (January 2011) *Envisional Ltd* <http://documents.envisional.com/docs/Envisional-Internet_Usage_Report-Summary.pdf>.

3 *Viacom International Inc v YouTube Inc*, Plaintiffs' Memorandum, 8 (Case No 1:07-cv-02103, SDNY, 2012).

copyrights.[4] Although unauthorised content appears to be declining with the growth of legitimate services,[5] digital piracy remains widespread. The intermediaries responsible for routing, storing and processing these data deny responsibility for policing infringements, citing the impracticability of monitoring and their inability to adjudicate claims of infringement, while internet users fear disproportionate interferences with privacy, internet access and innovation.

This chapter analyses the secondary liability of intermediaries for copyright infringement. Like chapter 4, it is not concerned with primary wrongdoing and does not set out to offer a substantive critique of copyright's primary rights or underlying policies. Section 1 examines the two main forms of secondary liability in copyright: authorisation and joint tortfeasorship. Section 2 analyses their application to intermediaries, observing that, like 'publication' in defamation actions, copyright is beginning to develop built-in limitations which shield network-layer intermediaries from monetary liability. Although these are welcome developments, the adversarial model of copyright enforcement remains unsuited to tackling widely dispersed, low-value digital infringements. Statutory interpretation provides limited guidance to courts because in many instances copyright legislation reflects a position characterised by deliberate ambiguity and inarticulate compromise.[6] Judicial procedures are slow to adapt, unwieldy and costly, and remove important questions to largely policy-agnostic institutions. In these circumstances, doctrines of secondary liability can provide only limited corrective outcomes.

Section 3 evaluates one alternative which requires ISPs to participate in enforcing copyright against their subscribers: first, by forwarding and recording allegations of infringement; and second, by taking technical measures to disconnect or suspend the accounts of repeat infringers. This section makes two arguments. First, properly administered, a notification regime may provide a proportionate and effective system of enforcement. Although imperfect, such a system is preferable to market-based alternatives and embodies a pragmatic, distributive enforcement strategy that complements the corrective framework analysed in sections 1 and 2. Second, proposed technical obligations remain mired by a degree of uncertainty and political discretion that is highly unsatisfactory; it is doubtful whether their uncertain benefits outweigh their numerous economic and social costs. This chapter concludes that they should be abandoned as disproportionate, unnecessary and incompatible with European law.

---

4 Robert Layton and Paul Watters, 'Investigation into the Extent of Infringing Content on BitTorrent Networks' (April 2010) *Internet Commerce Security Laboratory* <http://afact.org.au/research/bt_report_final.pdf>.

5 Sandvine Inc, *Global Internet Phenomena Report* (2012) 19 (BitTorrent traffic declined from 17.2 to 11.3 per cent).

6 *Stevens v Kabushiki Kaisha Sony Computer Entertainment* (2005) 224 CLR 193, 207–8 (Gleeson CJ, Gummow, Hayne and Heydon JJ).

1 The scope of secondary liability for copyright infringement

Copyright is now a creature of statute.[7] As such, the scope of property rights enjoyed by copyright owners — and the limits of others' liability for their infringement — fall to be determined foremost by legislation. Section 16(2) of the *Copyright Act* provides that:

> Copyright in a work is infringed by a person who without the licence of the copyright owner does, *or authorises another to do*, any of the acts restricted by the copyright.[8]

The copyright owner (or its exclusive licensee) has a statutory cause of action against anyone who infringes its copyright.[9] Relevantly, the acts restricted by copyright include copying a work — for example, by storing it 'in any medium by electronic means'[10] — and communicating it to the public by electronic transmission.[11] The meaning of these acts in digital environments has been the subject of extensive judicial[12] and academic[13] treatment. This chapter does not examine the liability of parties who engage in restricted acts by reason of their own conduct;[14] nor does it examine so-called 'secondary infringements' which arise from certain dealings with infringing articles[15] — both being examples of primary liability.

Instead, this section considers two doctrines which allow liability to be attributed for secondary wrongdoing: authorisation and joint tortfeasorship. Their effect is to augment the boundaries of responsibility beyond the defendant's own exercise of the acts restricted by copyright to encompass acts committed by third parties. The following sections consider the scope of these doctrines and their application to internet intermediaries.

1.1 The meaning of authorisation

The clearest mechanism by which one person may become liable for the infringing acts of another is when that person 'authorises another to do' the relevant acts. This formulation dates to the

---

7 *Donaldson v Becket* (1776) 1 ER 835, 839. See now *Copyright Act* s 171(2).

8 ('*Copyright Act*') (emphasis added).

9 Ibid ss 96(1), 101(2).

10 Ibid ss 16(1)(a), 17(2).

11 Ibid ss 16(1)(d), 20(2).

12 See, eg, *QC Leisure [No 3]* [2012] FSR 12 (Kitchin LJ) (communication to the public); *The Newspaper Licensing Agency Ltd v Meltwater Holding BV* [2012] RPC 1 (copying).

13 See, eg, Tilman Lüder, 'The Next Ten Years in EU Copyright: Making Markets Work' (2007) 18 *Fordham Intellectual Property, Media & Entertainment Law Journal* 1, 21–8; Bernt Hugenholtz et al, *The Recasting of Copyright & Related Rights for the Knowledge Economy* (2006).

14 Eg, if a website operator selects and uploads images or videos which are unauthorised copies, the acts giving rise to liability are committed by it alone.

15 See, eg, *Copyright Act* ss 23–26, 184(1)(b), 296ZG(2).

Copyright Act 1911 (Imp),[16] which defined copyright to include the exclusive right to engage in various restricted activities 'and to authorise any such acts as aforesaid'.[17] Once enacted, authorisation liability became a 'separate species' of infringement that existed in parallel with theories of direct infringement, joint tortfeasorship and vicarious liability.[18] It is one of 'a range of concepts and devices' from the *1911 Act* to survive in modern legislation.[19]

The meaning of authorisation has undergone a long and 'tortuous' evolution.[20] Like the concept of publication, its meaning has been progressively enlarged in response to new technologies for reproducing and disseminating information — in particular, creative and industrial works — followed by periods of contraction and rebalancing. In copyright cases, that evolution can be divided into three main phases: during the first, authorisation liability was almost non-existent, with courts recognising only a form of limited vicarious liability that required a relationship of agency with the primary infringer; following the 1911 amendments, courts focussed on *control over the place* of infringement by retail intermediaries; more recently, as manufacturers armed domestic infringers with reproduction technologies, concepts of authorisation began to emphasise *control over the means* of infringement. Relatively few cases have considered the liability of internet intermediaries. This makes it important to consider this evolution in some detail.

(a) *Early case law: relationship with the primary infringer*

Until the *1911 Act*, statutory liability attached to those who engaged in the infringing activity or 'caused' it to occur.[21] In practice, only its most direct causes were liable. Thus, in *Russell v Briant*, Wilde CJ described liability as confined to one who 'by himself or his agent ... actually takes part in a representation which is a violation of copyright.'[22] This was essentially a limited doctrine of vicarious infringement under which a defendant could be liable only for the acts of his servants

---

16 The phrase was first used in the Australian *Copyright Act 1905* (Cth) ss 13(1) (which described the right to 'authorize another person to do' the acts comprising copyright). See also ss 14(1) (dramatic and musical works), 34 (artistic works).

17 *Copyright Act 1911* (Imp) s 1(2) ('*1911 Act*').

18 Jane Ginsburg and Sam Ricketson, 'Inducers and Authorisers: A Comparison of the US Supreme Court's *Grokster* Decision and the Australian Federal Court's *KaZaA* Ruling' (2006) *Columbia Public Law & Legal Theory Working Papers*, Paper 0698, 10.

19 Robert Burrell, 'Copyright Reform in the Early Twentieth Century: The View from Australia' (2006) 27 *Journal of Legal History* 239, 239.

20 *WEA International Inc v Hanimex Corporation Ltd* (1987) 17 FCR 274, 285 (Gummow J) ('*WEA*').

21 See, eg, *Dramatic Literary Property Act 1833* (3 & 4 Will IV, c 15) s 2 (infringement by one who shall 'represent or cause to be represented' a work without consent); *Copyright Act 1842* (5 & 6 Vict, c 45) s 21.

22 [1849] 8 CBR 836; 137 ER 737, 742.

and agents. Simply to supply 'some of the means' of infringement — such as premises or equipment — was insufficient. To similar effect, *Karno v Pathé Frères* refused to extend liability to sellers of cinematograph films who knew they would be tortiously exhibited by third parties. The trial judge commented that the claim 'ought to have been brought, not against the defendants, but against the actual proprietors of the piratical performance impugned'. [23] Such a narrow approach to causation reflected a view of infringement in which secondary liability had little room to operate.

(b) *Actions against theatre proprietors and vendors: control over the place*

By abandoning 'cause' for 'authorise', the *1911 Act* widened the ambit of secondary liability. Its object was plainly 'to sweep away' decisions such as *Karno*.[24] Thus, one writer argued that

> the new Act has enlarged the protection accorded to the owner of a copyright by thus making it part of his monopoly to 'authorise' any of the acts referred to ...[25]

However, academic opinion was divided[26] and early cases interpreted authorisation liability narrowly. In *Performing Right Society Ltd v Ciryl Theatrical Syndicate Ltd*, Scrutton LJ considered that the words inserting authorisation 'are superfluous and add nothing to the definition' of copyright,[27] a view repeatedly endorsed.[28] Just two years later, an identically-constituted Court of Appeal held, on facts virtually indistinguishable from *Karno*, that the defendant film vendor was liable for authorising infringing screenings by a third party cinema.[29] Only Atkin LJ directly addressed the meaning of authorisation; Bankes and Scrutton LJJ concluded that the trial judge's findings were justified on other grounds.[30] In *obiter*, Bankes LJ observed that resort might be had to the 'ordinary dictionary sense of "sanction, approve, and countenance"';[31] Atkin LJ preferred the narrower sense of 'to grant or purport to grant ... the right to do the act complained of'.[32] Later courts are therefore correct to prefer the view of Atkin LJ, regarding *Falcon* as decided on

---

[23] *Karno v Pathé Frères* (1909) 100 LT 260, 262 (Vaughan Williams J) ('*Karno*').

[24] *Falcon*, 491 (Bankes LJ), 496 (Scrutton LJ).

[25] Walter Copinger, *The Law of Copyright* (5th ed, 1915) 136..

[26] See, eg, E J Macgillivray, *The Copyright Act, 1911: Annotated* (1912) 22 (arguing that the references to authorisation 'appear to be superfluous' and 'unnecessary').

[27] [1924] 1 KB 1, 10–11 (Bankes LJ), 12 (Scrutton LJ), 15 (Atkin LJ) ('*Ciryl*').

[28] See *Performing Right Society Ltd v Mitchell and Booker (Palais de Danse) Ltd* [1924] 1 KB 762, 773 (McCardie J) ('*Mitchell*').

[29] *Falcon v The Famous Players Film Co Ltd* [1926] 2 KB 474 ('*Falcon*').

[30] Ibid 491 (Bankes LJ), 496–7 (Scrutton LJ) (deciding the appeal on the narrower basis of primary infringement).

[31] Ibid 491 (Bankes LJ).

[32] Ibid 499 (Atkin LJ).

the basis that one who hires out a film to a cinema 'plainly' purports to grant the right to screen the film.[33]

One policy reason for the courts' willingness to impose liability onto proprietors and vendors was the relative difficulty of bringing suit against the nomadic and impecunious parties who exhibited infringing performances: 'A band', it was said, 'is often a migratory thing, and an action against it only might be of small avail to the plaintiffs.'[34] In other words, where it was difficult to identify and proceed against primary wrongdoers, the intermediary stood in a better position to avoid — and, if necessary, compensate — the copyright owner's loss. However, the criterion described in *Falcon* proved difficult to apply,[35] and later decisions oscillated between the available definitions.[36] Despite disagreement about its scope, authorisation liability came to be accepted as derivative in nature and conceptually distinct from the primary infringer's liability.[37] This follows from the statutory language — which requires the 'do[ing]' of one of the restricted acts — and from the fact that if the primary actor's conduct is not tortious or never actually takes place, there can be no actionable wrong in authorising it.[38]

(c) *Actions against manufacturers of machines: control over the means*

A trio of cases in the early 1980s rejected attempts to hold manufacturers and sellers of cassette recording equipment liable for acts of copying by purchasers.

(i) *A&M Records*[39]

In the first case, a claim against a manufacturer of blank cassette tapes was struck out as disclosing no cause of action. Their customers' mischief was 'home taping', which closely resembles the modern phenomenon of internet file-sharing: both technologies offer individuals a cheaper alternative with an 'extremely slender' chance of detection by the copyright owner;[40] in both instances, copyright owners sought to deploy authorisation liability to regulate those who

---

33 *CBS Inc v Ames Records & Tapes Ltd* [1982] Ch 91, 110 (Whitford J).

34 *Mitchell*, 765 (McCardie J).

35 See Hugh Laddie, Peter Prescott and Mary Vitoria, *The Modern Law of Copyright and Designs* (2nd ed, 1995) 911 (the formula 'countenance, sanction, approve' replaces 'one vague expression by another equally vague one').

36 See, eg, *Evans v Hulton & Co* (1924) 131 LT 534, 535 (Tomlin J); *Monckton v Pathé Frères Pathephone Ltd* [1914] 1 KB 395, 403 (Buckley LJ); *A & M Records*, 9–10 (Foster J) (countenance, sanction, and approve). Cf *Ames*, 106 (Whitford J) (grant of a right).

37 *Ash v Hutchinson and Co (Publishers) Ltd* [1936] 1 Ch 489, 497 (Slesser LJ), 502 (Romer LJ), 506–7 (Greene LJ) ('*Ash*').

38 *Mitchell*, 773 (McCardie J).

39 *A & M Records Inc v Audio Magnetics Incorporated (UK) Ltd* [1979] FSR 1 ('*A&M Records*').

40 *CBS Inc v Ames Records & Tapes Ltd* [1982] Ch 91, 99 (Whitford J) ('*Ames*').

supplied technologies that enabled copying. Despite the defendant's provocative advertisements, which depicted various infringing uses of tapes, Foster J held that there was no evidence that it had authorised any specific act of infringement.[41]

(ii) *Ames*

The second case targeted the operator of retail record stores from which members of the public could borrow audio recordings and purchase discounted blank tapes in return for a subscription fee. Whitford J held that the defendant was not liable for infringing copies members made from loaned records because it had not purported to grant any right to engage in unauthorised home taping.[42] The Court cast aside the broad 'countenance, sanction, and approve' definition of authorisation, preferring the narrower view of Atkin LJ in *Falcon*. The defendant had only supplied source material and not equipment or premises;[43] further, although it knew that borrowers may copy the cassettes, it did not grant permission to do so, instead warning borrowers to the contrary. In these circumstances, no inference of authorisation could be drawn.

(iii) *CBS v Amstrad*[44]

In the third case, the House of Lords held that neither the manufacturer nor retailer of dual-deck tape recorders had authorised infringements by purchasers who used them to duplicate commercial recordings without permission. Again, the defendants had issued various 'hypocritical and disingenuous' advertisements extolling the virtues of their devices,[45] which could duplicate tapes at twice the ordinary speed. Although usually accompanied by a small copyright disclaimer, they were intended to encourage purchasers to copy copyright-protected cassettes,[46] and the defendants knew the devices would 'inevitably' be used for that purpose.[47] Despite this, both the Court of Appeal and House of Lords rejected authorisation liability and endorsed Atkin LJ's narrow test of authorisation.[48] Lord Templeman placed particular emphasis on the manufacturer's lack of control over how its devices would be used, comparing Amstrad to the lending library in

---

41 *A&M Records*, 9–10 (Foster J).

42 Ibid 118. Like *iiNet*, the claimants relied on evidence from private investigators who conducted 'trap' purchases: at 104. Cf *RCA Records v All-Fast Systems Inc*, 594 F Supp 335 (1984) (where the defendant also supplied the retaping machine on its premises).

43 Cf *The University of New South Wales v Moorhouse* (1975) 133 CLR 1, 13 (Gibbs J), 23 (Jacobs J).

44 *CBS Songs Ltd v Amstrad Consumer Electronics plc* [1988] 1 AC 1013 ('*CBS*').

45 Ibid 1050 (Lord Templeman).

46 *Amstrad Consumer Electronics plc v The British Phonographic Industry Ltd* [1986] FSR 159, 171–2, 186–7 (Whitford J) ('*Amstrad v BPI*').

47 Ibid 189 (Whitford J).

48 Ibid 207 (Lawton LJ), 211 (Slade LJ), 217–18 (Glidewell LJ); *CBS*, 1054–5 (Lord Templeman) (Lord Keith, Lord Griffiths, Lord Oliver and Lord Jauncey agreeing).

Ames. Simply to condone and even deliberately encourage an infringing act was not to authorise it, unless accompanied by conduct which suggested some authority to grant the permission required for infringing use. Consistently with *Falcon*, lenders and sellers would not authorise copying because they lacked control over primary wrongdoers and did not purport to grant any permission to do the acts complained of.

Notably, these cases rejected attempts to pin liability on intermediaries using the tort of negligence.[49] Instead, they repeatedly affirmed the general principle that a person is not ordinarily under a duty to control another to prevent him from causing economic loss to a third party (here depreciation to the value of a *chose in action*). Although one person can clearly be liable in negligence for damage deliberately inflicted by another,[50] such duties arise in 'limited circumstances'.[51] Similarly, the courts refused to recognise a general duty not to infringe — which would be an illegitimate parallel duty to the statutory torts[52] — or not to facilitate a customer's infringement — which would be 'unsatisfactory' and 'far too heavy a burden'.[53] Such a conclusion seems beyond doubt: to hold otherwise would extend liability in negligence for pure economic loss far beyond established principles[54] and fracture the coherence of doctrines of joint tortfeasorship. In refusing to recognise an action for negligent facilitation, these decisions made clear that (outside limited cases of joint tortfeasorship) tort law will not assist a copyright owner to whom Parliament has not given a remedy.[55]

1.2 Joint tortfeasorship

Although copyright infringement sounds in a statutory remedy, it is a tort[56] to which common law principles of joint tortfeasorship apply just as they do to all other torts.[57] The two recognised connecting factors are procurement and common design. These are not independent torts, but

---

49 *Amstrad v BPI*, 213–14 (Slade LJ), 219 (Glidewell LJ). The reasoning in *Ames* appears to have assumed that no action lay for negligently facilitating a third party's infringement of copyright: see *Paterson Zochonis Ltd v Marfarken Packaging Ltd* [1983] FSR 273, 296 (Robert Goff LJ) ('*Paterson Zochonis*').

50 See *Dorset*, 1030 (Lord Reid), 1060 (Lord Diplock).

51 *Paterson Zochonis*, 299 (Robert Goff LJ).

52 Ibid 285 (Oliver LJ), 288 (Fox LJ).

53 Ibid 290 (Fox LJ), 301 (Robert Goff LJ).

54 Cf *Caparo Industries plc v Dickman* [1990] 2 AC 605, 634, 642–3 (Lord Oliver) (Lord Ackner agreeing), 655 (Lord Jauncey); *Muirhead v Industrial Tank Specialities Ltd* [1986] QB 507, 528–9 (Robert Goff LJ), 534 (Nourse LJ).

55 *Amstrad v BPI*, 214 (Slade LJ).

56 *WEA*, 283 (Gummow J).

57 *CBS*, 1058E (Lord Templeman); *MCA Records*, 424 (Chadwick LJ). See above chapter 3, § 1.3.

instead create joint liability for the primary infringement.[58] Joint liability might also arise based upon principles of agency and vicarious liability, though the principles are unsettled and excluded from this research.[59]

(a) *Procurement*

As explained in chapter 3, it is 'well established'[60] that A, an intermediary, is liable as a joint tortfeasor for procuring copyright infringements carried out by B.[61] The modern test has its genesis in *CBS*, where Lord Templeman explained that procurement is both causative (A's 'inducement, incitement or persuasion' must cause B's infringing act) and intentional (A must intend or ratify B's infringing act).[62] This bears some resemblance to inducement theories of secondary infringement recognised abroad.[63] On the facts, procurement failed because purchasers infringed of their own accord, not because they were persuaded by advertisements; Amstrad's conduct therefore made no causal contribution to the infringements.[64] Further, the act of procurement must relate to a specific infringement and not be 'at large'.[65] This sets a high bar for claimants who wish to pursue the providers of technologies used for large-scale infringement; to plead and prove each primary infringement is usually impracticable, as it was in *CBS* and *A&M Records*.

Procurement is also said to require incitement, which requires the secondary wrongdoer to have 'made himself a party to the infringement'.[66] The authorities do not clarify precisely what this involves, but, as argued in chapter 3, it appears to involve an assumption of responsibility for *infringing* uses of technology. This is a high threshold. Merely supplying the equipment, even with knowledge and intent that it be used tortiously, is insufficient if it is capable of both infringing and non-infringing uses. For such dual-use technologies, the only 'party' to the infringement is

---

58 *Unilever*, 608 (Mustill LJ); *MCA Records*, 418 (Chadwick LJ); *Belegging*, 66 (Buckley LJ); *Lumley*, 213 (Erle J).

59 *iiNet (HCA)*, [100] (Gummow and Hayne JJ). See above chapter 1, § 4.3(a).

60 *Newzbin*, [103] (Kitchin J).

61 *Ash*, 508 (Greene LJ); *Unilever*, 603 (Mustill LJ) (Ralph Gibson and Slade LJJ agreeing).

62 *CBS*, 1058 (Lord Templeman).

63 See, eg, *Metro-Goldwyn-Mayer Studios Inc v Grokster Ltd*, 545 US 913, 935–6 (2005).

64 'Cause' should be understood in the sense of belonging to a set of conduct sufficient for the primary infringement to occur: see, by analogy, Richard Wright, 'The NESS Account of Natural Causation: A Response to Criticisms' in R Goldberg (ed), *Perspectives on Causation* (2011) 285, 291. Cf Hart and Honoré, above n 14 (ch 3), 112; Tony Honoré, 'Necessary and Sufficient Conditions in Tort Law' in D G Owen (ed), *Philosophical Foundations of Tort Law* (1990) 363.

65 A similar approach prevails in the United States: see *Viacom v YouTube*, 15; *Perfect 10 Inc v CCBill LLC*, 488 F 3d 1102 (9th Cir, 2007); *Corbis Corp v Amazon.com Inc*, 351 F Supp 2d 1090, 1108 (WD Wash, 2004).

66 *Amstrad v BPI*, 212–13 (Slade LJ), 219 (Glidewell LJ). See also *Dunlop Pneumatic Tyre Co Ltd v David Moseley & Sons Ltd* [1904] 1 Ch 612, 620 (Stirling LJ), 621 (Cozens-Hardy LJ).

the individual who chooses to engage in the infringing uses. This is consistent with the view that, copyrights being monopolies in restraint of trade, they should not be given *de facto* enlargement by holding third parties liable for 'acts short of infringement'.[67]

(b) *Common design*

The second connecting factor is participation in a common design. As discussed in chapter 3, this refers to agreed or concerted action to carry out tortious acts (here infringing the copyright). Several issues arise in relation to intermediaries.

(i) *Threshold of participation*

Common design presents a higher threshold than authorisation, since the defendant must agree to participate in the infringing scheme and, though the agreement may be tacit,[68] cannot arise by indifference or omission. Initially, the threshold of participation was high: in *Lyon v Knowles* a share in the proceeds of an infringing production was insufficient for a theatre proprietor to be jointly liable with its lessee without capital contributions or 'joint action or control over the performances'.[69] Now any shared economic interest in infringement may suggest a common design, and even that is unnecessary.[70] Further, the agreement need not be express: the existence of a contract between an intermediary and third party infringer is 'irrelevant' unless its terms contemplate infringement.[71]

(ii) *Existence of non-infringing uses*

In *CBS*, Lord Templeman concluded that the defendant did not act in pursuit of a common design partly because its recording devices were dual-use machines. Purchasers' decisions to engage in the infringing uses were their own and not referable to any agreement.[72] This reflects the principle that simply supplying a lawful 'means' of infringement is insufficient. For similar reasons, an independent IT consultant is not liable for supplying and installing computer hardware subsequently used to upload infringing material.[73] Conversely, supplying a service which has no

---

67 *Amstrad v BPI*, 206 (Lawton LJ).

68 *Unilever*, 608 (Mustill LJ).

69 (1863) 3 B & S 556, 563; 122 ER 209, 213 (Cockburn CJ) ('*Lyon*'); aff'd (1864) 5 B & S 751; 122 ER 1010.

70 *Macaulay v Screenkarn Ltd* [1987] FSR 257, 259 (Falconer J).

71 *Grower v British Broadcasting Corporation* [1990] FSR 595, 611 (Knox J). Logically, if a contractual provision prohibits the infringing acts, this should be one factor militating against the existence of a common design.

72 *CBS*, 1055, 1057 (Lord Templeman) (Lord Keith, Lord Griffiths, Lord Oliver and Lord Jauncey agreeing).

73 *Magical Marketing Ltd v Holly* [2009] ECC 10, [60] (Norris J).

lawful uses may suggest a common design to engage in the unlawful ones.[74] In *Douglas*, a magazine editor commissioned photographs of the claimants in circumstances where the photographer would necessarily have to use unlawful means to fulfil the commission.[75] This was enough to make the magazine and editor engaged in a common design with the photographer to interfere with the claimants' privacy. This arrangement was unlike the 'lawful provision of lawful facilities' in *CBS*.

2 Application to internet intermediaries

Both doctrines of secondary copyright liability have been applied to application- and network-layer intermediaries. This section first examines cases involving platforms, hosts and ISPs, before speculating on the potential liability of gateways and marketplaces. Second, it evaluates whether these doctrines recognise appropriate limits on intermediary liability.

2.1 Platforms

The cassette recording cases substantially narrowed the scope of authorisation liability faced by intermediaries. By insisting upon an express or implied grant of a right to engage in the infringing activity, these decisions made even deliberate or calculated facilitation insufficient. Whether the alleged authorisation consists of goods sold (as in *Amstrad*) or ongoing subscription services (as in *Ames*), all conduct short of purporting to grant permission cannot support an authorisation claim. Importantly, the decision in *CBS* did leave open the prospect that such a grant can be implied from the circumstances and conduct of the defendant — a possibility readily taken up in three later cases involving website operators.

(a) *Newzbin*[76]

As the leading authority, *Newzbin* suggests a broad, multi-factor approach to authorisation by application-layer services. The defendants operated Newzbin.com, which compiled 'reports' identifying and aggregating files hosted on third parties' Usenet servers. Premium members (who

---

[74] See *Douglas v Hello! Ltd [No 2]* [2003] EMLR 28, 598 (Rix LJ).

[75] Ibid 598 (Rix LJ).

[76] *Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] FSR 21 ('*Newzbin*').

paid a subscription fee) could find and download files in a single bundle known as an 'NZB' package, which obviated the need to download hundreds of smaller archives and formed the 'crucial element' of the service.[77] The defendant claimed the index was 'content agnostic', but the vast majority of reports (greater than 99.7 per cent) related to infringing cinematograph films, software and other copyright works. Although Newzbin had copyright policies and warnings, it did not filter protected works; warnings were 'entirely cosmetic' and mere 'window dressing'.[78] Its operators knew that infringement was widespread. However, none of the infringing material was actually hosted by Newzbin and it could not directly control which files its members chose to access.

Despite purporting to adopt the narrow grant-based test of authorisation, Kitchin J applied a broad multi-factor test of implied authorisation, and regarded the Australian authorities (which, until *iiNet (HCA)*, preferred Bankes LJ's synonym test) as 'entirely consistent' with English principles.[79] While 'mere enablement, assistance or even encouragement' is insufficient, Newzbin had authorised infringement having regard to five factors. First, although not decisive, it had an ongoing contractual relationship with primary infringers. Second, it created and supplied the 'means of infringement', a sophisticated NZB browsing interface whose structure and features were directed at locating and copying copyright works. Third, when used as intended, the NZB facility 'inevitably' infringed copyright. Fourth, Newzbin maintained control over its use, which could be terminated at any time. Finally, despite knowing that most content infringed copyright, it did not take any steps to filter or discourage reports of copyright material. In these circumstances, Kitchin J inferred

> that a reasonable member would deduce from the defendant's activities that it purports to *possess the authority to grant any required permission* to copy any film that a member may choose from the Movies category on Newzbin ...[80]

Although liability may be the appropriate result on these facts, to impose it on the basis that members would wrongly assume a permission to copy where none in fact existed has the appearance of fiction. Given the low cost of membership and the website's many references to copied material, it seems doubtful whether anyone but the most naive members would assume Newzbin possessed any more authority to grant permission than they did themselves. Certainly, this is consistent with evidence of members' concern at being personally identified: they knew all

---

77 Ibid 522 (Kitchin J).

78 Ibid 526, 537 (Kitchin J).

79 Ibid 540 (Kitchin J).

80 Ibid 543 (emphasis added).

too well that what they were doing was *unauthorised* by the relevant copyright owners. Moreover, it may lead to absurd results: if a website dealing exclusively in pirated content states prominently that it possesses no authority to grant a licence to copy the works referenced there, the operator should still clearly be liable.

This scenario is better dealt with using joint tortfeasorship. In *Newzbin*, the website's structure, contents and design signalled a common design to infringe the claimants' copyrights; the defendant also 'induced' its editors to include meticulous listings of copyright works, guided members to the location of particular works and profited from subscription fees.[81] Because the service *inevitably* caused infringing copies to be made, unlike the tape recorders in *CBS*, and Newzbin knew infringement was widespread, the inescapable inference was that Newzbin made itself party to its members' infringing acts.[82] Although the claimants could not adduce evidence of specific infringements by particular members, this was only because the defendant retained no records of transmissions. Kitchin J made clear that this was not fatal to a finding of joint tortfeasorship but merely one factor to be considered.[83] This reflects a pragmatic concession to the traditional rule.

(b) *Dramatico*[84]

In this case, the liberal view of authorisation recognised in *Newzbin* was applied to hold the operators of a notorious BitTorrent tracker, The Pirate Bay ('TPB'), liable for authorising infringements by their United Kingdom users. Since this was also a case concerning authorisation by supply of hyperlinks to infringing materials, Arnold J referred to the same five factors as Kitchen J. Again, TPB supplied a 'comprehensive service' which allowed its users to search for and download torrent files using BitTorrent. The Court characterised the torrent files as the means of infringement, since — analogously to NZB files — they allowed the many fragments of a copyright work to be reassembled; this means the defendant supplied.[85]

Further, infringement was both inevitable and intended by TPB, as suggested by its name, mission statement and provocative media comments. The existence of non-infringing material was assumed to be trivial. As to control, TPB could prevent infringement by removing torrent

---

[81] Ibid 545–6 (Kitchin J).

[82] See Simon Baggs and Rachel Barber, '*A Changing Tide in the Fight against Online Piracy: How Significant is the* Newzbin *Judgment?*' [2010] *Entertainment Law Review* 234, 237.

[83] *Newzbin*, 545–6 (Kitchin J).

[84] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch), [81] (Arnold J) ('*Dramatico*').

[85] Ibid [75]–[77] (Arnold J).

files, which it did on occasion for other harmful materials, but chose not to do 'as a matter of policy' for copyright materials. The operators took no steps to prevent infringement, instead assisting users to circumvent blocks instigated by their ISPs. Arnold J held that these facts 'go far beyond' mere assistance, and satisfied both the broad and narrow tests of authorisation.[86] The case was, as Arnold J noted, even stronger than *Newzbin*.

Again, however, it seems difficult to describe TPB's service as a purported grant of authority to copy, though clearly procurement and common design. Like *Newzbin*, TPB's operators structured their website around infringement and profited from doing so. Common design therefore provides another basis for liability: the inescapable inference from their facilities having no (or *de minimis*) non-infringing uses was that they agreed their users could infringe. Arnold J accepted the 'induce, incite or persuade' test from *Newzbin* and held that TPB's operators were also jointly liable as procurers.[87]

(c) *Cooper*[88]

In this Australian decision, cited with approval in *Newzbin*, the operator of a website linking to MP3 files of the applicants' musical works was held to authorise users' infringements. The Court rejected an analogy with the manufacturers of blank tapes: Mr Cooper may not have had precise control over which files were accessed by users of his website, but he did have the ability to choose not to make the 'technical capacity' for infringement available and to design the website differently.[89] Respectfully, such a broad test of control makes the concept meaningless as a limiting criterion, since it would mean that any developer of a new technology has control in the loose sense that they could choose not to make the technology available. Although *Cooper* presents another clear example of calculated facilitation, it is again more properly classified as joint, rather than authorisation, liability, though the Court concluded that neither intermediary was a joint tortfeasor with end users for the puzzling reason that the index of hyperlinks was not edited or compiled by the defendants.[90]

---

[86] Ibid [81] (Arnold J).

[87] Ibid [83] (Arnold J).

[88] *Universal Music Australia Pty Ltd v Cooper* (2005) 150 FCR 1 ('*Cooper*').

[89] *Cooper v Universal Music Australia Pty Ltd* (2007) 156 FCR 380, 389 (Branson J).

[90] *Cooper*, 30–1 (Tamberlin J); aff'd (2007) 156 FCR 380, 393 (Branson J) (French J agreeing).

2.2 Hosts

No English cases have considered the position of those who host infringing materials. This is largely because, first, the storage safe-harbour has immunised those who do no more than store infringing material.[91] Second, notice-and-takedown procedures are now commonplace, leading hosts to remove obviously infringing content when requested. Third, the overwhelming majority of infringing material is stored in overseas jurisdictions where storage is cheaper and hosts less scrupulous. Injunctive relief in England may be difficult to enforce abroad.

Where hosting goes beyond passive storage, a host may be liable for authorising infringement. In *Cooper*, the host ('Comcen') assisted Mr Cooper to create the website, offered free hosting in exchange for advertising, and thereby enjoyed a commercial benefit from the high volume of infringing traffic it knew the website received.[92] The Court held Comcen liable as an authoriser because it was 'complicit in' the means of infringement,[93] took 'an active role' and had control.[94] This reasoning is subject to the criticism that the 'means' of infringement could be almost any antecedent technical condition, from computer hardware to electricity. It offers no principled criterion to limit the scope of authorisation liability. Further, like defamation cases, the distinction between an 'active' and 'passive' role remains unclear, but presumably requires more than a financial benefit, which almost all intermediaries receive.

2.3 ISPs

No English court has directly considered the *prima facie* liability of ISPs for authorising infringement by their users. However, the recent Australian decision in *Roadshow Films Pty Ltd v iiNet Ltd [No 3]* provides helpful guidance.[95] In that case, iiNet, a large retail ISP, was not liable for authorising its customers' BitTorrent downloads of the applicants' cinematograph films from third parties. The applicants argued that iiNet should be taken to authorise those infringements unless it took steps to warn or disconnect the relevant customers and remove infringing material from their computers.[96] In effect, they put their case as breach by omission of a statutory duty of care — the kind of duty previously rejected in *CBS*.[97] More than half of iiNet's internet traffic

---

91 *Lacoste v Multimania Production SA* [2001] ECC 22, 204 (a French case preceding the Directive).

92 *Cooper*, 20–1 (Tamberlin J).

93 *iiNet*, [398] (Cowdroy J).

94 *Cooper*, 29 (Tamberlin J).

95 [2010] FCA 24 ('*iiNet*').

96 *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16, [59] (French CJ, Crennan and Kiefel JJ) ('*iiNet (HCA)*').

97 *iiNet (HCA)*, [115] (Gummow and Hayne JJ).

consisted of such file-sharing. Although its customer agreement prohibited it, iiNet took no steps to disconnect or suspend customers whose accounts were implicated in notices sent by the applicants' investigators.

At trial, Cowdroy J dismissed the claim on various grounds, including that iiNet did not provide the actual means of infringement (BitTorrent) — over which it had no control — but merely an essential precondition (namely internet access). His Honour reread the Australian authorisation authorities as identifying the 'true means' of infringement: a party who provided a 'necessary precondition' to infringement would not be liable as an authoriser, whereas one who provided the actual 'means' would be.[98] Although this reasoning was properly rejected on appeal as unsupported by authority, the High Court of Australia unanimously agreed that iiNet had not authorised its subscribers' infringements.[99]

Like Cowdroy J, the majority judgment distinguished BitTorrent from other P2P distribution systems such as Grokster and KaZaA, twice observing that both BitTorrent and the internet had 'diverse' non-infringing uses[100] and that iiNet's services were not 'bound' to infringe.[101] While the provision of access was a necessary precondition of infringement, to download copyright materials via BitTorrent involved several additional steps: accountholders must first download a BitTorrent client, then find a `.torrent` file, connect to a tracker server such as TPB, locate peers, and download and reassemble file pieces. iiNet had no 'direct technical power' to prevent any of these activities. Further, it could not remove infringing material once downloaded or filter its retransmission.[102]

The plurality judgment of Gummow and Hayne JJ reached the same conclusion. Relying on *CBS*, their Honours emphasised that the makers of copying technology owed no duty 'to prevent or discourage or warn against infringement' and authorisation could not be repurposed to achieve that end.[103] Not only would such a duty be wide and uncertain, but it would be at iiNet's expense and would grant copyright owners a remedy (disconnection) which they could not have obtained in actions against primary infringers. Both judgments emphasised iiNet's minimal control over subscribers; while it could exercise 'attenuated' control by activating its contractual power to disconnect, it was not unreasonable to refuse to do so on the basis of incomplete

---

98 *iiNet*, [400]–[402] (Cowdroy J).

99 *iiNet (HCA)*, [38].

100 Ibid [18], [38], [64] (French CJ, Crennan and Kiefel JJ). See also *iiNet*, [411] (Cowdroy J).

101 Ibid [146] (Gummow and Hayne JJ).

102 Ibid [19–20], [65] (French CJ, Crennan and Kiefel JJ).

103 Ibid [115]–[116] (Gummow and Hayne JJ).

allegations, or to refuse to monitor their activities.[104] The majority accepted that evidence falling short of civil proof of infringement will not supply a reasonable basis for sending warning notices or disconnecting customers. To require an ISP to act on less 'assumes obligations … which the *Copyright Act* does not impose'.[105] Implicit in this reasoning is a judgment that ISPs should not be required to disconnect customers or undertake further investigation into allegations of infringement at their own expense.

The Court unanimously adopted Atkin LJ's formulation of authorisation, suggesting that Australian case law is reconverging on a standard approximating *CBS*. The narrower formulation in *Falcon* emphasises 'the immediacy … of the relationship between the primary infringement and the secondary infringement'.[106] In recasting authorisation liability in narrower relational terms, their Honours departed from use of synonyms, which illegitimately 'expand the core notion of "authorise"' by seizing upon a broader approximation of the word.[107] iiNet's supply of internet access did not involve any grant of a right to use the internet for tortious purposes; to the contrary, the customer agreement 'indicated iiNet's express, formal and positive disapproval' of such use.[108] Without 'direct power' to prevent the primary infringements, merely countenancing — even encouraging — them was insufficient.[109]

The *iiNet* first instance decision was cited with approval in *Newzbin*.[110] Despite obvious differences between the English and Australian tests of authorisation — in particular, s 101(1A) of the Australian *Copyright Act* — *iiNet* is a persuasive authority. If followed in England, it seems likely that, even when confronted with specific knowledge that a subscriber is using the internet to infringe copyright, an ISP will have no obligation to terminate access — at least until it has been presented with proof to a civil standard of infringement — and will not bear authorisation liability for infringements committed by its subscribers using tools supplied and controlled by third parties. In any case, the mere conduit safe harbour is likely to provide complete protection from monetary liability arising from transmission.[111] While this has been criticised as removing incentives to discourage infringement or adopt policies for dealing with persistent infringers,[112]

---

[104] Ibid [146] (Gummow and Hayne JJ).

[105] Ibid [75]–[78] (French CJ, Crennan and Kiefel JJ), [146] (Gummow and Hayne JJ).

[106] Ibid [127] (Gummow and Hayne JJ).

[107] Ibid [125] (Gummow and Hayne JJ). Moreover, the statutory factors specified in s 101(1A) of the *Copyright Act 1968* (Cth) suggested a narrower inquiry.

[108] Ibid [67] (French CJ, Crennan and Kiefel JJ).

[109] Ibid [69] (French CJ, Crennan and Kiefel JJ); citing *WEA*, 286–8.

[110] *Newzbin*, [95] (Kitchin J).

[111] See above chapter 3 § 2.1(a), chapter 4, §3.2(a).

[112] David Lindsay, 'Liability of ISPs for End-User Copyright Infringement' (2010) 29 *Communications Law Review* 1, 12.

the back-stop of tortious secondary liability should not be forgotten: tacit agreement or intentional inducement could still create liability. Section 3 explores one alternative scheme to regulate ISPs' non-monetary obligations.

2.4 Gateways

Even more limited guidance is available about the secondary liability of search engines and other gateways. Two general observations may be made on the basis of *CBS*, *Newzbin* and related decisions. First, it seems clear that a search engine which does no more than index generalist content, without emphasising specific infringing materials, will not authorise infringement by those who happen to access infringing content. Simply to direct users to available third party content is not to 'purport to grant … a right or licence' to copy it. Such search engines stand much closer to the position of a device manufacturer or lending library than to someone who specifically permits the infringing conduct: indeed, the search engine is generally not the tool with which the infringement takes place — merely a likely precondition of infringement — and not even an essential means (since the infringing materials could be accessed directly). To the extent infringing materials are themselves displayed in search engine snippets, the engine is arguably an automaton engaging in 'involuntary', non-tortious copying.[113]

Second, a search engine which is designed to index infringing material can be liable if its knowledge and technical control, coupled with indifference or inaction, 'reach a high degree from which authorization or permission may be inferred'.[114] Applying *Ames* and *CBS*, mere encouragement (for example, automatically generated search suggestions) or benefit may not be enough, but whether authorisation can be implied would ultimately be a question of fact.[115]

Some authorities suggest it is possible to form a common design by hyperlinking to a website which provides a service that 'inevitably' results in infringement. In *Football Dataco Ltd v Sportradar GmbH*,[116] a Gibraltan website operator linked to Sportradar's live football scores service, which incorporated data sourced from the claimants' databases. The website used the scores service to attract punters to its own sports betting website; it was presented as the default option and in such a way that infringement of the database rights was inevitable by anyone who

---

[113] See *Sony Music Entertainment (UK) Ltd v Easyinternetcafe Ltd* [2003] IP&T 1059, 1066 (Peter Smith J).

[114] *Ciryl*, 9 (Bankes LJ).

[115] *CBS*, 1054.

[116] [2012] EWHC 1185 (Ch) ('*Sportradar*').

accessed it. Referring to this encouragement, Floyd J held that the website operator was not a 'mere intermediary, like eBay'; its activities went beyond facilitation and 'adopt[ed]' the acts of data extraction in pursuit of a common design with website users.[117] By contrast, Sportradar merely made the data available in Austria to website operators, which was insufficient to form a common design with English website users who accessed the data. Importantly, no party knew that its use of the service was tortious, which underscores that it is sufficient for an agreement to relate to *activities* rather than the specific commission of wrongdoing. However, it seems doubtful that hyperlinking alone could be sufficient inducement or agreement for joint liability.

2.5 Marketplaces

Courts in other jurisdictions have dismissed claims against credit card gateways because they have 'no direct connection' to infringement.[118] Simply making copying more probable or straightforward is an insufficiently material contribution for secondary liability; further, there is a strong public interest in insulating financial intermediaries from threats of liability for processing transactions.[119] The same result seems likely under the English doctrine of authorisation, since payment processors and auction websites generally do not grant the right to copy or use purchased matter in any particular way simply by acting as the vendor's agent. In particular, most marketplaces lack actual control over how their transaction systems are used, do not encourage or induce infringement and take no steps to promote it as a means of infringement. Certainly, this is consistent with Floyd J's description of eBay in *Sportradar*.

2.6 Preliminary conclusion

This examination of authorisation and joint tortfeasorship suggests that both concepts furnish useful corrective mechanisms in individual cases. Their development shares some parallels with the evolution of publication in defamation cases: all three doctrines operate as flexible levers to define limits on secondary liability; they have expanded to accommodate new technological intermediaries; they exclude conduit facilitators who lack a strong nexus with primary wrongdoing; their scope frequently hinges on knowledge and control. However, both doctrines suffer from four defects which make them unsuitable for demarcating effective and proportionate

---

[117] Ibid [84], [81] (Floyd J). This conclusion was upheld by the Court of Appeal following a reference to the CJEU: *Football Dataco Ltd v Stan James (Abingdon) Ltd [No 2]* [2013] FSR 30, [96]–[100] (Jacob LJ).

[118] *Perfect 10 Inc v Visa International Service Association*, 494 F 3d 788, 796 (9th Cir, 2007).

[119] Ibid 797–8.

limits on intermediary liability for internet copyright infringement: first, intrinsic ambiguity in the causal and relational thresholds required for liability; second, overlap and incoherence; third, inflexibility; and fourth, the absence of distributive tools needed to apportion responsibility. These concerns are now explained in turn.

(a) *Ambiguity*

First, the tests for authorisation and joint infringement lack certainty. They are meant to describe clear thresholds of conduct sufficient to justify imposing liability for the infringements of another. Those thresholds are, at best, vague and, at worst, circular and incoherent. The limits of authorisation are characterised by 'uncertainty and case-by-case assessment'.[120] Joint liability is an 'elusive question'.[121] As the Court observed of a joint defendant in *C Evans & Son Ltd v Spritebrand Ltd*, 'broad considerations of policy may be material in deciding on which side of the line his participation fell'.[122] In short, 'each case depends upon its own particular facts',[123] which entails a costly and lengthy trial. While this reflects the contestable nature of secondary liability, the tests applied are essentially circular, since they inevitably reduce to asking whether the secondary party

> has been personally involved in the commission of the tort *to an extent sufficient to render him liable* as a joint tortfeasor…[124]

Subsequent courts have pointed out the 'obvious' recursion this enquiry invites.[125] The reason, they suggested, was that secondary liability raises policy questions which require contextual, case-by-case resolution. In a sense, this is all these doctrines are *meant* to do: they elude precise definition yet furnish conceptual structures for analysing the causal and relational culpability of secondary actors in particular cases. However, like tests of 'proximity' and 'fairness' introduced to the modern law of negligence, these incremental, case-by-case tools are difficult to apply and provide little *ex ante* guidance to intermediary defendants.

---

[120] See Kimberlee Weatherall, 'Of Copyright Bureaucracies and Incoherence: Stepping Back from Australia's Recent Copyright Reforms' (2007) 31 *Melbourne University Law Review* 967, 994.

[121] *Mentmore Manufacturing Co Ltd v National Merchandising Manufacturing Co Inc* (1978) 89 DLR (3d) 195, 203 (Le Dain J).

[122] [1985] 1 WLR 317, 331 (Cumming-Bruce LJ) (O'Connor and Slade LJJ agreeing).

[123] *Wah Tat Bank Ltd v Chan Cheng Kum* [1975] AC 507, 515 (Lord Salmon).

[124] *MCA Records*, 418 (Chadwick LJ) (emphasis added).

[125] *Società Esplosivi Industriali SpA v Ordnance Technologies (UK) Ltd* [2008] RPC 12, 297 (Lindsay J).

(b) *Overlap and incoherence*

Although common design is conceptually distinct from procurement, there is 'considerable overlap' between them[126] and judges tend to treat them together[127] or as instances of a wider principle that A is liable as a joint tortfeasor wherever he makes B's infringement 'his own'.[128] Slade LJ described the inquiry as whether the defendant 'is actually a joint tortfeasor or has procured *or incited* such act',[129] suggesting a certain level of taxonomic confusion. Some cases simply use the terms interchangeably,[130] which is regrettable. Authorisation often turns on identical factors to joint tortfeasorship — as in *Dramatico* and *Newzbin* —which suggests some degree of redundancy. Indeed, the difference may only be significant where an intermediary is based abroad, since territorial limits placed upon the act of authorisation would exclude statutory liability[131] but perhaps not procurement from abroad of a tort in England.[132]

(c) *Inflexibility*

Doctrines of secondary infringement are binary measures of responsibility. Either a secondary defendant is liable to compensate the full extent of damage caused by the primary tortfeasors, or not at all. To prevent the injustice that might otherwise arise from imposing liability disproportionate to a defendant's participation, secondary infringement doctrines operate as normative gatekeepers; they prevent intermediaries from facing liability for contributory conduct which is insufficient to justify imposing full responsibility for the acts of others. Because joint liability offers no balancing mechanism once defendants are admitted within the gateway of liability, there is no guarantee of proportionality. This is especially problematic where the other tortfeasors are anonymous or judgment-proof. In these circumstances, it might be unfair to hold one intermediary liable for the full extent of the loss.

Equally, if the defendant's conduct falls short of this threshold, the claimant may be left without any remedy at all. When *Amstrad* was before the Court of Appeal, Nicholls LJ expressed

---

126 *Newzbin*, 543 (Kitchin J).

127 See, eg, *Dramatico*, [83] (Arnold J).

128 *Newzbin*, 545 (Kitchin J).

129 *Amstrad v BPI*, 212 (Slade LJ) (emphasis added). Presumably, his Lordship does not intend to treat procurement and incitement as separate categories distinct from joint tortfeasance.

130 *Nintendo Company Ltd v Playables Ltd* [2010] EWHC 1932 (Ch), [49]–[50] (Floyd J).

131 *Copyright Act* ss 16(1) (copyright the right to do specified acts 'in the United Kingdom'), 161(2) (applies 'to things done in the United Kingdom'). Cf *ABKCO Music v Music Collection International Ltd* [1995] RPC 657.

132 See *Coin Controls Ltd v Suzo International (UK) Ltd* [1999] Ch 33, 39–40 (Laddie J).

his 'profound dissatisfaction' at dismissing the claimants' appeal. Although the appeal was 'misconceived', the problem remained of intermediaries who

> are, on a large scale, inciting others to infringe copyright in circumstances where the copyright owners have no practical remedy against the actual infringers, and there is nothing the copyright owners can do through the courts to stop them. If, indeed, that is so, the present state of the law is, in my view, gravely defective.[133]

The same criticism can be made with even greater force of the widespread infringements occurring online today. In practical terms, there is very little copyright owners can do to stop them: as the High Court commented in *iiNet*, suing individual infringers would be 'somewhat impractical'[134] — a mere 'teaspoon solution to an ocean problem'.[135] While the answer is not *necessarily* to impose monetary liability on intermediaries, doctrines of secondary infringement fail to supply a sufficiently nuanced solution.

(d) *Lack of distributive mechanisms*

Authorisation and joint tortfeasorship lack the distributive mechanisms necessary to regulate internet infringement effectively. This is not a criticism of the doctrines themselves, which were never designed for this purpose, but it suggests they may be unsuitable for solving problems of internet copyright infringement. Various practical details are left unsolved: how, for example, detection and enforcement costs are to be shared; what is to prevent a disconnected infringer from shifting to another ISP; how to deal with mistaken allegations; what status is to be accorded the privacy and security of putative infringers' data, among others. While they may provide criteria for developing case-by-case liability standards, they do not aim to provide a comprehensive regulatory framework. Further, neither literalism nor Parliamentary intent will provide much assistance in construing the word 'authorise' from a 1911 statute in a dispute involving Twitter or Google.

Consequently, it should hardly be surprising that the default policy choices embedded in doctrines of secondary infringement are 'not readily suited' to large-scale internet claims involving vast numbers of tortfeasors.[136] Those choices cannot be made using dictionary definitions or by analogy with 19th century common law principles. For courts to bend doctrines of secondary infringement to this purpose risks introducing uncertainty and inconsistency into

---

[133] *CBS Songs Ltd v Amstrad Consumer Electronics plc* [1988] Ch 61, 78 (Nicholls LJ) (Fox LJ agreeing).

[134] *iiNet (HCA)*, [55] (French CJ, Crennan and Kiefel JJ).

[135] Randal Picker, 'Copyright as Entry Policy: The Case of Digital' (2002) 47 *Antitrust Bulletin* 423, 442; cited in *In re Aimster Copyright Litigation*, 334 F 3d 643, 645 (7th Cir, 2003) (Posner J).

[136] *iiNet (HCA)*, [79] (French CJ, Crennan and Kiefel JJ).

other areas of secondary liability, especially if these changes occur mainly in egregious rather than borderline cases. Conversely, courts already possess extensive powers to regulate non-monetary liability in far more nuanced ways, as discussed in chapters 6–8. Ultimately, Parliament is in a better position to address questions of monetary liability in a manner which properly reflects the delicate balance embedded in copyright law. Section 3 accordingly considers recent a legislative scheme that was introduced with this objective.

3 Graduated response obligations

Wielding a powerful rhetoric of artists as victims, piracy as theft and intermediaries as free-riders,[137] copyright owners have pressured regulators to supply more effective remedies to combat online infringement. These attempts to alter the 'legal and procedural "rules of the game"' have proven highly successful,[138] culminating in a worldwide shift towards non-monetary enforcement schemes. These take many forms, ranging from private notice-and-notice agreements to statutory 'three strikes' regimes such as the *Digital Economy Act 2010* (UK) ('*DEA*'). Their common element is that ISPs are required to take some action against users accused of infringing copyright.[139] Underlying concerns about their necessity, proportionality, and compatibility with human rights are two basic questions: the extent to which intermediaries should be compelled to internalise the costs of infringement; and the legitimacy of non-monetary penalties levied upon subscribers, such as disconnection.

This research does not address the second question. Instead, it evaluates the *DEA* from the perspective of intermediaries. First, this section outlines ISPs' obligations under the scheme. Second, it compares the scheme's benefits and costs. Finally, it assesses the scheme's proportionality and compatibility with safe harbours and general limits on copyright remedies. This section argues that, although improved disclosure and enforcement procedures are desirable, the *DEA*'s proposed technical obligations suffer from such serious defects that their benefits are unlikely to outweigh their economic and social costs, while the effectiveness of its notification scheme should be monitored once implemented. Ultimately, judicially-mediated disclosure,

---

[137] See generally Peter Yu, 'Digital Copyright and Confuzzling Rhetoric' (2011) 13 *Vanderbilt Journal of Entertainment and Technology Law* 881.

[138] Yana Breindl and François Briatte, 'Digital Network Repertoires and the Contentious Politics of Digital Copyright in France and the European Union' (Paper presented at the Oxford Internet Institute conference, Oxford, 16 September 2010) 6.

[139] Nicolas Suzor and Brian Fitzgerald, 'The Legitimacy of Graduated Response Schemes in Copyright Law' (2011) 34 *University of New South Wales Law Journal* 1, 1.

blocking and freezing remedies of the kind examined in chapters 6 and 7 are likely to supply more effective and proportionate remedies in many circumstances.

3.1 Overview

The *DEA* is a 'soft' mechanism for digital copyright enforcement that requires ISPs, rights-holders and an industry regulator (OFCOM) to operate a scheme by which primary infringers can be identified, educated and penalised. Graduated response originated as a theory of nuclear deterrence that recommended escalating nuclear payloads to defeat threats of aggression.[140] This forgotten relic of the missile age was revived largely by sustained lobbying[141] and the failure of ISPs and rights-holders to agree on self-regulatory anti-piracy measures.[142]

The scheme comprises three main components: first, the framework of regulatory powers and duties contained in the *DEA* itself; second, the Initial Obligations Code ('Code'),[143] in which OFCOM specifies details of the scheme's operation;[144] and third, ancillary statutory instruments, including a cost-sharing order and decrees issued by the Secretary of State.[145] While these instruments create obligations which are not 'duties' in the sense familiar to private lawyers and do not sound in 'liabilities' when breached, they represent a new class of 'soft' administrative obligations owed to regulators. This section argues that the *DEA* is a logical response to the politics of intellectual property that reflects a deliberate compromise between the interest structures of copyright owners, intermediaries and consumers. However, as a deliberate compromise, it leaves crucial features of the scheme undetermined and fails to clarify its relationship with existing remedies.

(a) *Scope of the scheme*

The scheme applies only to 'qualifying ISPs' — those with more than 400 000 fixed-line subscribers who obtain internet access 'under an agreement' and using an allocated IP address.[146] Mobile and wholesale ISPs are excluded — the former on the assumption that infringement is less

---

140 Lawrence Freedman, *Kennedy's Wars: Berlin, Cuba, Laos, and Vietnam* (2002) 93–4.

141 Peter Yu, 'The Graduated Response' (2010) 62 *Florida Law Review* 1374, 1400.

142 See, eg, *Gowers Review*, [5.92]–[5.100]. Cf *Creative Britain*, 50. See also BERR, 'Consultation Document on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing' (July 2008) 47.

143 OFCOM, *Online Copyright Infringement Initial Obligations Code* (2010) ('*Code*').

144 *Communications Act 2003* (UK) s 124D(1) ('*Communications Act*').

145 Online Infringement of Copyright (Initial Obligations) Cost Sharing Order 2010 (UK).

146 *Communications Act* s 124C(5); *Code* § 2.4.2; *DEA* s 124N.

prevalent[147] and more difficult to trace to individual subscribers;[148] the latter to ensure that hosts, backbone operators and application-layer platforms are not captured. The clear intention is that the scheme should apply only to large retail ISPs, sparing smaller businesses disproportionate costs of compliance. Although providers of wireless access — for example, in coffee shops, libraries and universities — will fall within the definition where service is provided under an agreement (and not gratuitously), most wireless ISPs would be unlikely to meet the quantitative threshold. Nevertheless, qualifying ISPs represent at least 93.5 per cent of the UK residential market for internet access.[149]

Only a 'qualifying copyright owner' may avail themselves of the scheme. These are copyright owners who have given advance warning of their intention to issue notices to ISPs and paid any required share of the anticipated enforcement costs.[150] Although any copyright owner (or its agent) may participate in the scheme,[151] in practice these requirements serve to confine its operation to repeat-player claimants in the music and film industries, further limiting the volume of complaints faced by qualifying ISPs.

(b) *Initial obligations*

The *DEA* divides ISPs' duties into two categories: the first, initial obligations arise upon the *Code* coming into force; the second, more onerous technical obligations start only once declared by the Secretary of State at least one year later. The initial obligations further divide into two duties.

(i) *To notify subscribers*

First, qualifying ISPs must send notifications to their subscribers whenever a valid copyright infringement report ('report') is received from a qualifying copyright owner in relation to a subscriber's IP address.[152] Reports are sent electronically in an agreed format, and must include various particulars of the work and its alleged infringement.[153] Unlike the notification standard in *ii*Net, copyright owners need not show proof to a civil standard — merely a belief that an

---

147 The main reasons are: (1) the higher cost of bandwidth to consumers; (2) *ad valorem* usage pricing; (3) latency and speed limitations; (4) network traffic management.

148 Most mobile networks assign addresses which may be shared between multiple subscribers, making identification much more difficult and unreliable.

149 OFCOM, *Online Infringement of Copyright and the* Digital Economy Act 2010*: Notice of Ofcom's Proposal to Make by Order a Code for Regulating the Initial Obligations* (26 June 2012) 33.

150 See *Code* § 2.1.

151 See *Code* § 1.

152 *Communications Act* s 124A(4); *Code* §§ 5.3, 5.6–5.9.

153 *Code* §§ 3.1, 3.3, 3.8.

infringement is occurring by means of the ISP's service. Upon receiving a valid report,[154] an ISP must contact the person to whom it relates with a standard form notice.[155] The form of notices is initially polite and educative, but becomes progressively sterner with each notification.[156] Their 'central purpose' is educational: to inform subscribers that their conduct is tortious and persuade them to change their behaviour.[157]

(ii) *To provide infringement lists*

Any subscriber who is sent three successive notifications within a 12 month period must be added to a copyright infringement list. This list records the details and number of reports made against each subscriber, without revealing their identity.[158] ISPs owe three basic obligations with respect to list data. First, they must maintain the list and delete a subscriber upon expiry of her earliest notification.[159] Second, they must supply the anonymised list on request to any qualifying copyright owner.[160] Third, they may be obliged by court order to disclose an uncensored copy of the list to a qualifying copyright owner. This appears to preserve *Norwich Pharmacal* disclosure, though its relationship with the *DEA* remains unclear.[161]

(c) *Technical obligations*

The government has indicated that it expects the initial obligations to reduce online infringement by 70 to 80 per cent,[162] a target widely considered optimistic.[163] If, as seems likely, the target is not met after 12 months, the Secretary of State can activate a second set of 'technical' obligations,[164] which require ISPs to adopt various measures to deter and prevent infringement by repeat infringers. To avoid the risk of obsolescence, the obligations themselves are left to a future technical obligations code.[165] Measures could include: per-subscriber *access restrictions* to

---

[154] *Code* § 4.3.

[155] *Communications Act* s 124A(6); *Code* §§ 5.6.2, 5.7.2, 5.11. This is unless a notice was already sent in the same calendar month, which prevents multiple notices being sent during a single incident.

[156] *Code* §§ 5.6–5.8, 5.13–5.14.

[157] *BT*, [233] (Parker J).

[158] *Communications Act* s 124B(2); *Code* § 6.4.

[159] *Communications Act* s 124B(3); *Code* § 6.1.

[160] *Communications Act* s 124B(1); *Code* § 6.2.

[161] See below chapter 6, § 4.3(f)(ii).

[162] Explanatory Notes, *DEA*, [62].

[163] See below § 3.2(a).

[164] *Communications Act* ss 124H, 124G(6). This would require new legislation and provision for appeals: OFCOM, *Notice of Ofcom's Proposal to Make by Order a Code for Regulating the Initial Obligations* (26 June 2012) [1.19].

[165] *Communications Act* ss 124I, 124J.

specified content or protocols (similar measures are examined in chapter 7);[166] *capping and traffic management*, which limit the volume and speed of data, both infringing and non-infringing, which subscribers may access;[167] and *suspension or termination* of a subscriber's access.[168] Little is known about the technical obligations at this stage.

(d) *Enforcement*

DEA obligations are enforced by OFCOM under a system of discretionary powers. It may direct ISPs and copyright owners to take specified remedial steps, impose civil penalties of up to £250 000 per contravention, and require payment of compensation to affected third parties.[169] Unlike private remedies, these penalties are neither compensatory nor restitutionary in nature, though they may include compensation. They are determined at first instance by administrative rather than judicial decision. Enforcement actions are brought by a public authority, OFCOM, rather than private claimants, and only after a process of investigation, notification and failure to take remedial action. Subject to one exception, only once a penalty is imposed do ISPs' obligations crystallise into a duty to pay money.[170]

The exception relates to enforcement costs, which are apportioned 75 per cent to copyright owners and 25 per cent to ISPs.[171] This distribution reflects a partial compromise between the 'polluter pays' principle — the idea that ISPs have been enriched by the stronger demand for bandwidth supposedly catalysed by the availability of infringing material — and the 'beneficiary pays' principle, which stresses that property owners should bear the costs of enforcing their private monopolies.[172] The legitimacy of imposing a copyright enforcement subsidy on ISPs and their subscribers is discussed below.

---

[166] *Communications Act* sub-ss 124G(3)(b), (d), 124G(4).

[167] *Communications Act* s 124G(3)(a).

[168] *Communications Act* s 124G(3)(c). See further BIS, *Digital Britain: Final Report* (June 2009) 113.

[169] *Communications Act* s 124L; *Code* §§ 9.20–9.22.

[170] *Code* § 9.27. Penalties are recoverable as debts.

[171] *Communications Act* s 124M; OFCOM, above n 149, [8.8].

[172] Department for Business, Innovation and Skills, *Online Infringement of Copyright (Initial Obligations) Cost Sharing: HM Government Response* (2010) 2.

(e) *Domain name registries*

The *DEA* contains backstop powers which enable the Secretary of State to assume control over 2LD domain name registries.[173] These powers are intrusive — effectively permitting nationalisation — but have been largely overlooked by commentators.[174] Although the measures formally apply to any 2LD registry that operates within a 'UK-related' TLD, such as `.co.uk`, only Nominet UK Ltd meets these criteria, so the provisions apply to a single private entity. They are triggered by a 'serious relevant failure': first, where 'the registry, or any of its registrars or end-users' misuse domain names in prescribed ways; or second, where the registry's complaint-handling procedures fail to comply with prescribed requirements.[175] Such a failure must be 'serious', in the sense of being likely to harm communications or the interests of the public.[176] It is suggested that these powers are unlikely ever to be exercised; instead, they provide a further example of the shift away from liability rules towards softer regulatory measures which create strong incentives for intermediaries to comply with government directives — in this case relating to domain name policy.

For present purposes, three features are noteworthy. First, a registry operator faces quasi-secondary liability for failures by 'any of its registrars or end-users'. Second, the scheme targets only the lowest-level domain intermediary, rather than registrars, resellers and registrants. This approach reflects an assumption that domain registries are more efficient loss-avoiders than downstream parties. Registries can, for example, introduce registration conditions in upstream licences and enforce them by seizing or cancelling domain names, indirectly preventing harm more effectively than the hundreds of English registrars or millions of registrants could compensate it. Third, the *DEA* envisages a more active policing role by registries, both under dispute resolution procedures (such as the Nominet DRP and UDRP) and by dealing pre-emptively with emerging threats to network security and consumer welfare.[177] These policing roles arguably 'deputise' registries in similar ways to ISPs, and signal a more active legislative role in the future development of the DNS.

---

[173] *Communications Act* ss 124P(2) (appointing a new manager), 124R(3) (altering constitution).

[174] See, eg, Joel Smith and Darren Meale, 'Legislative Comment: Internet — *Digital Economy Act 2010*' [2010] *European Intellectual Property Review* 75, 76.

[175] *Communications Act* s 124O(3).

[176] *Communications Act* s 124O(4).

[177] Registries must prohibit various practices and uses of domain names: see above n 162, [93]–[94].

3.2 Evaluation of benefits and costs

As a system designed to reduce claimants' enforcement costs, the *DEA* falls to be assessed on a cost–benefit basis. This section identifies several potential benefits, but their magnitude is uncertain compared to the serious overall costs of compliance. Caution is therefore warranted until the impact of the initial obligations on ISPs and subscribers can be properly assessed.

(a) *Benefits*

Supporters of the *DEA* claim it will deter infringement, simplify enforcement, provide certainty to ISPs, and deliver a fair and impartial system for determining copyright complaints involving intermediaries. The government estimates total gains at £1.2bn over ten years.[178] However, upon closer examination many of these benefits appear doubtful or rest on untested assumptions.

(i) *To claimants*

Three main benefits to copyright owners may be identified. First, notification provides a simpler and more targeted method of reducing internet infringement than legal actions against primary or secondary infringers. A decade of end-user litigation has demonstrated its inability to deter insolvent, anonymous and profligate defendants.[179] Even clear verdicts against intermediaries such as Newzbin and TPB can be illusory: replacements emerge, Hydra-like, while the unsuccessful defendant has meanwhile vanished into the mists of the internet, leaving the claimant to bear its costs and, like Sisyphus, begin enforcement anew.

If notification is effective, claimants would no longer need to sue their customers — a practice which has made recording labels 'the most hated industry since the tobacco industry'.[180] As Parker J commented in *R (British Telecommunications plc) v Secretary of State*, infringement lists are a 'more efficient, focussed and fair system', since they allow claimants to decide which primary infringers are worth pursuing.[181] By focussing on the most active infringers, claimants can maximise the ratio of expected remedies to enforcement costs. However, the scheme ultimately relies on threats of sanctions against individual subscribers to be effective. If subscribers realise proceedings will not be instituted even against egregious infringers, the prophylactic effect of

---

[178] BIS, *Impact Assessment for the* Digital Economy Act 2010 (April 2010) 55.

[179] See Kristina Groennings, 'Costs and Benefits of the Recording Industry's Litigation against Individuals' (2005) 20 *Berkeley Technology Law Journal* 571, 589–90.

[180] Steve Knopper, 'RIAA's Gaze Turns from Users to ISPs in Piracy Fight' (*Rolling Stone*, 19 December 2008) <http://rollingstone.com/music/news/riaas-gaze-turns-from-users-to-isps-in-piracy-fight-20081219>.

[181] [2011] EWHC 1021 (Admin), [228] (Parker J) ('*BT*').

notices will quickly evaporate. Similarly, while receiving notices might function as a 'symbolic reminder' of copyright norms,[182] it might also have the opposite effect if notices could be ignored without sanction.

Second, there is some evidence that sending notices to subscribers would materially reduce infringement levels. Although the evidence is divided, one English survey reported that 70 per cent of respondents would stop infringing after receiving one notice; another 16 per cent upon receiving a second.[183] This is consistent with two claimant-commissioned studies suggesting that a majority of consumers would stop downloading films if warned not to do so — 71 per cent in New Zealand,[184] 81 per cent in Germany.[185] However, a more recent English survey suggests only 33 per cent would respond to warnings without any threat of sanctions.[186] Empirical evidence suggests at least some positive impact: the French authorities claim a 26 per cent reduction in infringing P2P activity,[187] while South Korea reports a 70 per cent reduction after each successive notice.[188]

These findings are supported by theory. As Yu observes, notification (backed by effective threats of sanctions) can deter infringement in a similar way to the accrual of demerit points for drunk driving or speeding.[189] Such sanctions alter users' calculus of wrongdoing to increase the expected value of penalties for infringement. Although the expected cost of infringing behaviour could not be raised to a point sufficient to deter all infringement or dissuade sophisticated users from evading detection, this is not the objective: the *DEA* only needs to maintain reasonable compensation for copyright owners. The fact that recidivist infringers can evade the system is not fatal to its efficacy unless evasion becomes widespread. Accordingly, Parker J's conclusion in

---

[182] Yu, above n 141, 1383.

[183] Entertainment Media Research Ltd, *Digital Entertainment Survey* (2008) 13.

[184] New Zealand Federation Against Copyright Theft, 'One Warning Will Stop Most Youth from Infringing Movies Online' (Press Release, 20 October 2009). See Commerce Committee, Copyright (Infringing File Sharing) Amendment Bill (119-2) (2010) <http://parliament.nz/enNZ/PB/SC/Documents/Reports/8/3/6/49DBSCH_SCR4901_1-Copyright-Infringing-File-SharingAmendment-Bill.htm> 6.

[185] IFPI, *Digital Music Report* (2012) 17.

[186] Entertainment Media Research Ltd, *Digital Entertainment Survey* (2009) 149.

[187] IFPI, above n 185, 17. Cf Sylvain Dejean, 'Une Première évaluation des Effets de la loi Hadopi sur les Pratiques des Internautes Français' (March 2010) <http://marsouin.org/IMG/pdf/NoteHadopix.pdf> (showing increase in file-sharing after HADOPI); Brett Danaher et al, 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France' (January 2012) <http://electronlibre.info/IMG/pdf/HADOPI-IFPI-FINAL.pdf> (showing no significant effect in legal sales).

[188] Ed Baden-Powell and Luke Anthony, 'Case Comment: Digital Economy — Act 2' (2012) 23 *Entertainment Law Review* 130, 132.

[189] Yu, above n 141, 1381–2. Olivier Bomsel and Heritiana Ranaivoson, 'Decreasing Copyright Enforcement Costs: The Scope of a Graduated Response' [2009] *Review of Economic Research on Copyright Issues* 13, 27.

BT that the *DEA* 'may well have [a] positive effect' seems at least plausible.[190] Nevertheless, the extent of its effectiveness remains speculative.

Third, claimants point to economic analysis suggesting that the *DEA* will reduce their enforcement costs by providing a subsidised system for identifying and preventing wrongdoing.[191] The three suggested improvements are: first, a reduced need for litigation due to deterrent effects; second, where this prophylaxis proves insufficient, the availability of cheaper procedures to pursue primary wrongdoers; and third, a system for identifying the most egregious wrongdoers over time. The benefits resemble those of the UDRP, which aims to provide a cost-effective procedure to determine allegations of cybersquatting, which, like allegations of P2P infringement, are overwhelmingly well-founded.[192] Like the *DEA*, decisions are enforced by intermediaries (registrars) and unsuccessful parties may appeal. Conversely, *DEA* determinations do not rest on jurisdiction by consent and are merely preliminaries to an actual claim. This argument also rests on an assumption about effectiveness: if end-user litigation remains necessary, there is no reason to suppose that overall costs would be any lower; if anything, they would be higher due to the added delay and cost of sending notices.

(ii) *To intermediaries*

Although intermediaries face new obligations and potential liability under the *DEA*, they benefit in three ways. First, the scheme offers standardised processes which reduce the overall costs of receiving and processing notifications. Because infringement reports are currently received in incompatible formats and media, ISPs must manually review thousands of daily notices; under the *DEA*, reports will be submitted electronically in a standardised XML format.[193] OFCOM will also supply a specification for matching IP addresses to subscribers and guidance on appropriate evidentiary standards. Following this guidance reduces ISPs' reputational and legal risk compared to self-regulation.

Second, the scheme reduces the pressure on all intermediaries to supply monetary remedies for infringement. While participation does not confer immunity from authorisation liability —

---

[190] *BT*, [233] (Parker J). Cf Robert LaRose et al, 'Sharing or Piracy? An Exploration of Downloading Behavior' (2005) 11 *Journal of Computer-Mediated Communication* 1 (showing that social outcomes and other factors more likely to influence file-sharing choices).

[191] See Bomsel and Ranaivoson, above n 189, 22–3.

[192] See WIPO, 'Case Outcome by Year(s) (Breakdown)' (2012) *Arbitration and Mediation Center* <http://wipo.int/amc/en/domains/statistics/outcome.jsp>.

[193] *Code* § 4(6)(a)(ii); OFCOM, *Notice*, 43. It is unclear whether qualifying copyright owners will be prohibited from sending notices outside the scheme. If they are not, ISPs may need to retain legacy processes, which will remove many of the benefits of standardisation.

and therefore cannot be considered a safe harbour[194] — it is evidence of reasonable steps being taken to discourage infringement, which makes an inference of authorisation or joint wrongdoing less likely. Further, the scheme encourages cooperation between ISPs and claimants which may remove the impetus for litigation.[195] Finally, repeat infringers and infringing content disproportionately account for bandwidth utilisation.[196] An effective graduated response system therefore promises appreciable reductions in ISPs' network traffic and operating costs, without necessarily impacting consumption patterns and revenues from non-infringing customers. Further, ISPs commonly bundle internet access with lawful video and music services. Reducing infringement, it may assumed, would benefit those services.

(iii) *To subscribers*

The *DEA* offers four main benefits to internet users. First, because it encourages claimants to pursue targeted action rather than indiscriminate litigation against any suspected infringer, users are less likely to be threatened with legal action. Litigation is focussed on serial offenders, who have received prior warnings.[197] This approach avoids catching infringers unawares, who then face a 'mafia-like choice' between costly settlement and costlier litigation[198] — a problem further discussed in chapter 6 — by making it less likely that casual infringers or innocent subscribers are threatened with proceedings without prior warning. Second, the scheme educates infringers — many of whom are likely to be minors — allowing households to put in place appropriate measures to self-regulate their children's internet usage without immediate exposure to liability. Although often overlooked, this critically important function helps avoid the generation of 'copyright criminals' feared by Lessig.[199] Third, reduced infringement levels may benefit non-infringers by increasing network performance[200] and affording access to a higher quality and variety of copyright materials.[201]

---

[194] Cf Yu, above n 141, 1384.

[195] Suppose, for example, that graduated response was used to deter cassette copying in the 1980s: retailers kept registers of customers and copyright owners carried out surveillance to detect infringing tapes. Those responsible were reported to stores, who had to educate and, if necessary, refuse supply. Whatever other criticisms could be made of such a scheme, it would be much less likely to produce litigation resembling *CBS*.

[196] See Benoît Felten and Herman Wagter, 'Do Data Caps Punish the Wrong Users?' (28 November 2011) *Diffraction Analysis* <http://www.fiberevolution.com/2011/11/do-data-caps-punish-the-wrong-users.html> (finding that the top 1 per cent of users account for 20 per cent of bandwidth consumption).

[197] *BT*, [228] (Parker J).

[198] Lawrence Lessig, *Free Culture* (2004) 51; Yu, above n 141, 1390.

[199] Lawrence Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy* (2008) xvii.

[200] See, eg, Yu, above n 141, 1385.

[201] BIS, above n 178, 69.

Finally, the Act and *Code* specify minimum standards for disclosure and basic processes for identification, which reduce the likelihood of users' personal information being wrongfully disclosed to claimants. As a universal statutory scheme, rules are mandatory and identical as between ISPs, which promotes transparency and consistency. Further, OFCOM and any appeal bodies are subject to judicial review and must act compatibly with human rights. These guarantees far exceed what a privately administered scheme would offer.

(b) *Costs*

The *DEA* also carries substantial economic, social and technological disadvantages, which are analysed below under the same headings.

(i) *To claimants*

As noted above, the *DEA* may not actually be effective in materially reducing infringement. Even if it is, claimants still bear the onus of detecting and notifying ISPs of alleged infringements. Currently, most repeat-players outsource these tasks to digital forensics firms, who employ automated monitoring tools to generate and send millions of notices each week. Because claimants must pay a per-notice fee, this will limit their ability to report infringements to ISPs. Even to maintain current levels of notifications would cost most claimants £5m annually,[202] though this may serve to deter frivolous or unverified complaints.

Second, *DEA* notification procedures are protracted. Unlike *Norwich Pharmacal* orders, which may be sought immediately from a single instance of *prima facie* infringement, the process for producing and disclosing infringer lists is lengthy and eventually requires claimants to go through the same process to obtain disclosure. Finally, claimants may incur indirect costs from curtailing infringement. Strict enforcement may simply reduce the overall consumption of copyright works, thereby causing greater long-term harm to cultural industries.[203]

(ii) *To intermediaries*

ISPs will incur various costs in establishing and operating the system: in particular, receiving reports; matching reports to subscribers; generating and sending notices; retaining records; compiling infringer lists; handling subscribers' inquiries about notices; maintaining data security;

---

[202] Ibid 77 (based on industry estimates of £460,000 per million reports and 10.75 million reports per year).

[203] See Sylvain Dejean, Thierry Penard and Raphaël Suire, 'The French "Three Strikes Law" against Digital Piracy and the Change in Usages of Pirates' (Paper presented at Internet, Politics, Policy 2010, Oxford, 16 September 2010) 3–5, 13.

and monitoring compliance.[204] Technical measures would involve 'far more burdensome technical obligations'[205] and additional implementation and operational costs. All costs are highly sensitive to changes in the scheme's efficacy:

> Compliance cost figures are very sensitive to the underlying assumptions. If only 50% instead of 70% of infringers stopped, annual costs of compliance would increase from a range of £6–20 million to a range of £10–30 million. If instead of one letter [claimants] required two letters a year to be sent to serious infringers, the costs would double.[206]

To meet these variable costs, OFCOM has proposed a notification fee payable by each qualifying copyright owner equal to 75 per cent of the relevant costs. However, a fixed fee encourages incomplete investigation of complaints, and leaves ISPs with the variable risk of customer complaints. In the short term, making ISPs bear a percentage of costs may cause them to resist all efforts to make the *DEA* succeed or proceed to technical obligations, which is likely further to reduce the scheme's overall efficacy, potentially increasing overall costs.

ISPs have also criticised the quantitative threshold as distorting the market for internet access by encouraging infringers to shift to smaller or mobile ISPs who are exempt from *DEA* obligations and able to offer lower-cost services. This issue was considered and dismissed by the Court of Appeal in *BT*, principally because there was no evidence this was likely to occur.[207] Switching costs associated with early contractual termination and reconnection make market distortions unlikely, especially given the price-sensitivity of infringers as a consumer group.

(iii) *To subscribers*

The greatest costs are borne by internet users. First, users are likely to pay ISPs' share of enforcement costs by way of higher access fees. This may widen the 'digital divide and exclude marginal consumers from affordable broadband access.[208] Second, using IP address evidence will inevitably produce false-positive notifications which harm innocent subscribers' interests. Flaws in IP address matching are widely acknowledged and have led to claims against inanimate

---

[204] *Code* § 33(4).

[205] Anne Barron, '"Graduated Response" *à l'Anglaise*: Online Copyright Infringement and the *Digital Economy Act 2010*' (2011) 3 *Journal of Media Law* 305, 341.

[206] BIS, above n 178, 71. The government estimated total costs for all stakeholders at '£290–500 million' over five years: ibid 55.

[207] *BT* [2012] EWCA Civ 232, [111] (Richards LJ) ('*BT (CA)*'); *BT*, [201]–[202] (Parker J).

[208] Cf BIS, *Britain's Superfast Broadband Future* (2010) 5, 8–9, 14 (endorsing policy of universal broadband access).

printers,[209] deceased grandmothers,[210] children confined to hospital,[211] and copyright owners themselves.[212] There is an inherent tension between reducing enforcement costs for claimants and ensuring allegations of infringement are properly investigated, tested and judicially reviewed.[213] Glickman's infamous comment summarises one extreme: 'When you go trawling with a net, you catch a few dolphins.'[214] Because reports under the *DEA* are premised on mere assertions and honestly-held beliefs, the *Code* does not come close to requiring 'unequivocal and cogent evidence' of the kind necessary to succeed in civil proceedings.[215] Accordingly, it seems likely to catch some 'dolphins'.

Although false-positive notifications do not necessarily cause any immediate harm to subscribers (since individually they create no liability), they do place them at a forensic disadvantage in subsequent infringement proceedings because they may function as *prima facie* evidence of wrongdoing. Nevertheless, repeated allegations against a subscriber are intrinsically different to repeated judicial determinations of infringement. Possible solutions include increasing evidentiary standards; imposing penalties for reckless or dishonest allegations; requiring, by analogy with the rules in civil proceedings, claimants to bear all costs associated with an unsuccessful allegation;[216] and accrediting ISPs' and claimants' detection processes, as occurs in France.[217] However, because the ultimate question of infringement is not trivial to resolve,[218] even these steps will not completely eliminate errors. Perplexingly, hard-core infringers are probably better off, while non-infringers are worse off if they are mistakenly targeted or forced to subsidise the costs of investigating infringers.

---

[209] See Michael Piatek, Tadayoshi Kohno and Arvind Krishnamurthy, 'Challenges and Directions for Monitoring P2P File Sharing Networks — or Why My Printer Received a DMCA Takedown Notice' (Paper presented at 3rd USENIX Workshop on Hot Topics in Security, San Jose, 29 July 2008).

[210] See, eg, Andrew Orlowski, 'RIAA Sues the Dead' (5 February 2005) *The Register* <http://theregister.co.uk/2005/02/05/riaasuesthe-dead/>.

[211] See, Steve Ragan, 'RIAA Sues Hospitalized Girl — Court Issues Default Judgment' (9 December 2008) *Tech Herald* <http://thetechherald.com/articles/RIAA-sues-hospitalized-girl-court-issues-default-judgment/>.

[212] *Viacom International Inc v YouTube Inc*, Defendants' Memorandum, 15 (Case No 1:07-cv-02103, SDNY, 2012).

[213] See *iiNet* [2011] FCAFC 23, [205]–[211] (Emmett J) ('*iiNet (Full Court)*').

[214] See Cory Doctorow, 'Online Censorship Hurts Us All' (*The Guardian*, 2 October 2007) <http://guardian.co.uk/technology/2007/oct/02/censorship>.

[215] *iiNet (Full Court)*, [210] (Emmett J). Given that many ISPs receive up to 30,000 notices per week — figures which can be expected to rise under the *DEA* — and recover fixed costs, they have few incentives (other than possible reputational damage in the eyes of customers) to test the accuracy of claimants' allegations.

[216] Suzor and Fitzgerald, above n 139, 24–5. Presumably this would include the subscriber's legal expenses on an indemnity basis.

[217] OFCOM, *Notice*, above n 149, 12.

[218] *iiNet*, [115]; cf *iiNet (Full Court)*, [402] (Jagot J (dissenting)).

Third, the scheme reverses the onus of proof: alleged infringers are presumed tortfeasors, unlike court proceedings.[219] Subscribers must pay a £20 fee to appeal any notice, unless they succeed.[220] Finally, the *DEA* increases uncertainty about which informal dealings with copyright will continue to be tolerated. Many tortious but trivial infringements are not enforced by copyright owners, usually they cause minute damage, are prohibitively costly to prevent, or actually benefit the copyright owner.[221] Katyal argues that there is a 'pervasive divide' between what copyright law requires and what the market tolerates.[222] Graduated response does not distinguish between 'technical' infringements and more serious incursions; this threatens to prevent informal dealings with copyright which are tolerated and socially beneficial. The quantitative threshold is too low to accommodate these practices meaningfully.[223]

3.3 Proportionality

Proportionality is a basic component of the rule of law[224] and limits copyright remedies against intermediaries both under EU law and within the *DEA* itself.[225] In *BT*, Parker J described a two-stage inquiry: first, to identify the legitimate aim of the provisions; and second, to determine whether 'the legislator unlawfully failed to balance the relevant interests at stake.'[226] In his Lordship's view, the Court should be slow to interfere because the Act reflects Parliament's considered answer to 'a major problem of social and economic policy'.[227] The Court concluded that the initial obligations were not disproportionate, a finding not disturbed on appeal.[228]

Parker J's approach to judicial review can only be described as 'highly deferential'.[229] It fails to assess whether the relative weighting given to each interest was appropriate,[230] and so avoids

---

[219] William Patry, *Moral Panics and the Copyright Wars* (2009) 13.

[220] *Code* § 38.

[221] Tim Wu, 'Tolerated Use' (2007) 31 *Columbia Journal of Law & the Arts* 617, 619–20. Cf Yafit Lev-Aretz, 'Second Level Agreements' (2012) 45 *Akron Law Review* 137, 139–40 (arguing that most such uses are actually authorised under bulk derivative-work licences negotiated between copyright owners and content platforms).

[222] Sonia Katyal, 'Filtering, Piracy Surveillance and Disobedience' (2009) 32 *Columbia Journal of Law & Arts* 401, 418.

[223] See John Tehranian, 'Infringement Nation: Copyright Reform and the Law/Norm Gap' [2007] *Utah Law Review* 537, 547.

[224] *R (Alconbury Developments Ltd) v Secretary of State for the Environment, Transport and the Regions* [2001] 2 AC 295, [51] (Lord Slynn); Lord Hoffmann, 'A Sense of Proportion' in Andenas and Jacobs (eds), *European Community Law in the English Courts* (1998) 149, 156.

[225] See Enforcement Directive art 3(2); Framework Directive art 3(1)(a); *DEA* s 124J(1)(g).

[226] *BT*, [243] (Parker J).

[227] *BT*, [211] (Parker J).

[228] *BT (CA)*, [76]–[77] (Richards LJ) (Arden and Patten LJJ agreeing).

[229] Barron, above n 205, 335.

[230] *Contra R (Daly) v Secretary of State for the Home Department* [2001] 2 AC 532, [27] (Lord Steyn).

assessing the underlying policy that it more closely resembles traditional *Wednesbury* review than a proportionality analysis. In a scheme whose net effect hinges upon complex economic and behavioural evidence, this offers limited scope for challenging assumptions made by Parliament which, although wrong, are not irrational or wholly without basis. A less deferential approach will be taken here, asking whether the chosen means was 'necessary' (in the sense of whether any less intrusive alternatives exist),[231] and whether it actually strikes a *fair* balance between the competing rights of copyright owners, intermediaries and individuals.[232]

(a) *Legitimate aim*

In seeking to reduce infringement and protect claimants' property rights, the *DEA* clearly pursues a legitimate aim. Those rights are recognised as fundamental rights.[233] However, it is worth noting that this aim needs to be assessed in light of the wider objectives and policies of the copyright system: stronger exclusive rights encourage underutilisation, which carries social costs, as does spill-over from excessive enforcement. Eventually, those social costs to society as a whole will outweigh the benefits of stronger protection to copyright owners.[234]

(b) *Assessment of chosen means*

The essence of proportionality is an assessment of means and ends.[235] Any policy which desires to achieve some aim must be capable of achieving it (adequacy), be necessary in a democratic society (or, in some cases, *strictly* necessary) to achieve it, and not cause disproportionate harms relative to what it does achieve.[236] It follows that proportionality is intrinsically linked to how effective a policy is at achieving the desired end.[237] It is, in other words, an 'equitable ratio'[238] — a *rationabilitias*.[239] In light of this, assessment of the *DEA* largely depends on how well it performs

---

[231] *Viagogo (CA)*, [25]–[29] (Longmore LJ). Cf *BT*, [258] (Parker J).

[232] *Scarlet*, [42]–[46]; *Promusicae*, [61]–[68]

[233] *Charter* art 17(2); *Convention* First Protocol, art 1.

[234] Identifying that threshold falls outside this research. See Suzor and Fitzgerald, above n 139, 14.

[235] Nicholas Emiliou, *The Principle of Proportionality in European Law: A Comparative Study* (1996) 23–4.

[236] Jürgen Schwarz, *European Administrative Law* (revised ed, 2006) 687. See also Juan Cianciado, 'The Principle of Proportionality: The Challenges of Human Rights' (2010) 3 *Journal of Civil Law Studies* 177, 179–80.

[237] Schwarz, above n 236, 679.

[238] Marius Andreescu, 'Principle of Proportionality, Criterion of Legitimacy in the Public Law' (2011) 18 *Lex ET Scientia* 113, 118.

[239] Cianciado, above n 236, 178.

once implemented and, in particular, its economic side-effects.[240] Because the initial and technical obligations carry distinct consequences, they are considered separately.

(i) *Initial obligations*

Most objections to the notification scheme fall under one of four headings. First, the scheme is said to be ineffective. The French experience is revealing though ultimately inconclusive: of 736,000 notices sent,[241] 62,000 subscribers have received a second notice and 165 have received a third.[242] It is difficult to infer any deterrent effect from these data, since many notice recipients have reported obfuscating and continuing their infringing activity, though music sales and profits appear to have stabilised.[243] Nevertheless, the ends likely to be achieved by the scheme are inconclusive, and will require close evaluation once implemented.

The second objection relates to subscribers who are themselves intermediaries — for example, where the primary infringements were committed by family members, guests, customers or unauthorised users of a wireless network.[244] It is correct that, absent something more, simply allowing someone to access a connection, or failing to secure it properly, is unlikely to be authorisation or joint tortfeasance. However, no direct liability attaches to being placed on an infringer list, and in a subsequent action for infringement the Court would apply ordinary liability rules (exonerating such a subscriber). Further, a statutory defence applies where a subscriber can show she was not the infringer and took 'reasonable steps' to secure her connection.[245] This objection is therefore unconvincing, since the scheme does not expand tortious liability beyond existing limits.

The third category of objections identifies possible 'chilling effects', such as subscribers refraining from non-tortious activities for fear of being placed on an infringer list,[246] and access points — such as coffee shops, libraries and hotels — ceasing to offer open access. In *BT* Parker J was not persuaded that these were credible prospects because, as noted above, claimants would

---

[240] Susan Kiefel, 'Section 92: Markets, Protectionism and Proportionality — Australian and European Perspectives (2010) 36 *Monash University Law Review* 1, 15.

[241] See Le Monde, 'L'Hadopi Veut Envoyer Jusqu'à 2000 Mails par Jour d'Ici la Fin de l'Année' (26 October 2010).

[242] Marc Rees, 'La Montée en Puissance de la Hadopi en Trois Graphiques' (18 January 2012) *PC INpact* <http://pcinpact.com/news/68390-hadopi-volume-email-lettre-recommandee.htm>.

[243] See IFPI, *Digital Music Report 2013* (February 2013) 5–6 ('An industry on the road to recovery').

[244] See, eg, Martin Kretschmer et al, 'Statement on Constitutional Aspects of the Digital Economy Bill' (1 April 2010); Yu, above n 141, 1426'; Open Rights Group, 'Digital Economy Act' (1 December 2012) <http://openrightsgroup.org/issues/deact>.

[245] *DEA* s 124(K)(6).

[246] See, eg, Suzor and Fitzgerald, above n 139, 11; Michael Boardman, 'Digital Copyright Protection and Graduated Response: A Global Perspective' (2011) 33 *Loyola of Los Angeles International and Comparative Law Review* 223, 235–6.

still need to prove that the access provider had authorised infringement — 'a relatively high test'[247] — and so no disproportionate liability would result. Existing liability rules already apply to such intermediaries without difficulty, and the quantitative threshold in the *Code* is likely to exclude them in any case. Similarly, non-tortious dealings with copyright by subscribers seem unlikely to be deterred:[248] exceptions and defences to infringement are recognised in subscribers' grounds of appeal. Moreover, most socially-valuable dealings occur on platforms that have takedown procedures which are cheaper and quicker than ISP notification, and therefore more likely to be used by claimants.

The fourth objection is to ISPs being required to subsidise the cost of enforcing private property rights at all. Under the scheme, ISPs must pay copyright owners despite making no recognised use of copyright material. This enlarges the statutory monopoly without corresponding social returns. Copyright owners respond that contributions are justified by ISPs' facilitation of infringement and the need to encourage efficient compliance.[249] Although this may be justified if ISPs benefited from wrongdoing,[250] it is not obvious that this is so, since ISPs would face comparable bandwidth costs if consumers sourced content legitimately.[251] The existence of enforcement duties does not necessarily mean ISPs should pay for those measures unless they are themselves secondary infringers. To require payment as a non-infringer is inconsistent with the approach taken to injunctions against other non-wrongdoers.[252]

Despite these criticisms, it seems difficult to sustain an objection to notification being carried out by ISPs under the supervision of administrative bodies. Repeated allegations of infringement over a substantial period are unlikely *all* to be false-positives, and the effect of a notice is not even *prima facie* liability, but rather to educate and deter. Provided costs are appropriately borne by copyright owners rather than innocent consumers or intermediaries, soft measures of this kind are preferable to inflexible claims under primary and secondary liability rules. Although imperfect, the *DEA* supplies adequate procedural guarantees to ensure that subscribers receive sufficient notice of allegations and time in which to read, act on and, if

---

[247] *BT*, [235]–[240] (Parker J).

[248] Alternatively, if they are, this suggests tortious dealings would be deterred at least as much.

[249] Barron, above n 205, 344–5.

[250] See Bomsel and Ranaivoson, above n 189, 22.

[251] Cf Annemarie Bridy, 'Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement' (2010) 89 *Oregon Law Review* 81, 87–8.

[252] See below chapter 7, § 4.5.

necessary, contest them before incurring liability. The notification scheme contained in the *DEA* accordingly reflects a fair balance between claimants', ISPs' and consumers' rights.

(ii) *Technical measures*

Technical measures are different. Wholesale disconnection from the internet is never a proportionate response to an allegation of copyright infringement, because it would violate subscribers' rights to private life and communications, protection of personal data and freedom of expression,[253] and ISPs' freedom to conduct a business.[254] This research does not directly consider the impact of disconnection upon subscribers, but instead notes four reasons why imposing technical obligations on ISPs would be disproportionate.

First, technical measures are penalties that would disproportionately affect non-tortious uses of the internet. Although certain criminal penalties can prevent non-criminal activities,[255] existing remedies for copyright infringement are mainly compensatory or restitutionary.[256] Disconnection represents a different *kind* of remedy; it is not a transfer of value designed to compensate or disgorge wrongdoing, but a means of denying the defendant access to information — akin to digital incarceration. In the terminology of layers, disconnection amounts to disabling the physical layer in order to regulate activity at the content layer. As Solum and Chung point out, this is inherently over-inclusive, since all communications — even those which do not fall within the regulatory purpose of disconnection — are prevented. Accepting such technical measures would necessarily be inconsistent with the end-to-end principle.[257] Indeed, in most cases, they would *predominantly* affect non-tortious activities, which the possibility of alternative access (in a library, workplace or with a smartphone) may be insufficient to ameliorate. Presumably for similar reasons, the High Court concluded in *ii*Net that disconnection would not be reasonable even if infringement had been proved, since it would disproportionately restrict lawful activities.[258]

Second, there is no necessary connection between the magnitude of infringement and the type of sanction applied. Minor home copying appears to count towards graduated response

---

[253] *Charter* arts 7, 8, 11. See La Rue, above n 107 (ch 1), [78].

[254] *Charter* art 16.

[255] Consider the disqualification of motorists for certain driving offences: *Road Traffic Offenders Act 1988* (UK) s 34. Although lawful driving is prohibited, this is to enforce the public interest in safe driving and not exclusively to protect private property rights.

[256] *Copyright Act* ss 96(2), 97(2) (aggravated damages and specific relief are also available in appropriate cases).

[257] See above chapter 2, § 3.2.

[258] *ii*Net, [250], [438] (Cowdroy J).

equally with commercial piracy and wilful self-enrichment. While any proportionate system of technical measures must align penalty with severity of wrongdoing, the *DEA* contains no such guarantee.[259] Indeed, it contains few details about when technical measures would be applied, for what duration, and by whom. Because their activation is a matter of largely ministerial discretion, ISPs could be held in a kind of regulatory purgatory under threat of technical measures. The Joint Committee on Human Rights criticised this 'skeletal approach' as inappropriate where powers could infringe users' fundamental rights, since there is no prospect of parliamentary scrutiny of their exercise.[260]

Third, there is no guarantee that technical measures would be imposed after determining questions of infringement under a 'prior fair and impartial procedure', as required by the Framework Directive.[261] This underscores the fact that ISPs — like other intermediaries — are in no position to evaluate allegations of infringement made by third parties in reliance upon limited and one-sided assertions of fact, or to exercise quasi-judicial power as censors or in applying penal sanctions.[262] Although the *DEA* does contain an appeal mechanism,[263] that is an essentially retrospective measure which reverses the onus of proof by requiring subscribers to appeal and supply evidence against adverse findings. Even if disconnection required a court order, as occurs in New Zealand and France,[264] it would still proceed on the basis of untested allegations rather than proof of wrongdoing, and fail to protect disconnected subscribers, who may thereby be deprived of access to the very information needed to bring an appeal.

Fourth, even assuming perfect detection and matching, there are doubts how effectively technical measures would operate. Without coordination via some kind of centralised 'blacklist', subscribers could immediately reconnect with another ISP. There is nothing to prevent parallel infringement via smartphones, which are serviced by non-qualifying ISPs. While a central subscriber registry would complete the analogy with driving demerit points, it would draw unwelcome comparisons with the identity registration requirements of autocratic states and only fuel concerns over 'network surveillance' and internet freedom.[265] Ease of circumvention is not

---

[259] See Suzor and Fitzgerald, above n 139, 16.

[260] Joint Committee on Human Rights, *Legislative Scrutiny: Digital Economy Bill* (HL Paper 44; HC 327) (5 February 2010) 3, 14.

[261] Directive 2009/140/EC [2009] OJ L 337/37, 46, art 1(1)(b); *Communications Act* s 124J(1)(g).

[262] See Suzor and Fitzgerald, above n 139, 22, 28. See also T R S Allan, *Constitutional Justice: A Liberal Theory of the Rule of Law* (2001) 11.

[263] *Communications Act* s 124K(2); *Code* §§ 7.1, 7.19.

[264] See *Copyright (Infringing File Sharing) Amendment Act 2011* (NZ) ss 122J, 122O, 122P; Loi n° 2009-1311 of 28 October 2009, *Projet de loi relatif à la protection pénale de la propriété littéraire et artistique sur internet* (FR) art 3.

[265] Nicola Lucchi, 'Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI)' (Unpublished paper no 11-07, 2010) 12.

conclusive of disproportionality, but it does reduce the ability of technical measures to achieve their stated aims.

The proportionality analysis requires copyright enforcement to be placed in perspective and weighed against other, perhaps more fundamental, rights and freedoms. However important copyright enforcement may seem to claimants, it comprises a relatively small part of most citizens' social and political lives. As the European Data Protection Supervisor concluded:

> While intellectual property is important to society and must be protected, it should not be placed above individuals' fundamental rights to privacy, data protection, and other rights such as presumption of innocence … and freedom of expression.[266]

These spill-over harms are simply 'too high a price for society to pay' for better copyright enforcement, even if disconnection is a measure of last resort.[267] Partly this is because it is unclear what is being bought: while claimants assert billions of pounds in losses, empirical evidence remains equivocal.[268] The zero-sum arithmetic proposed by copyright owners, which equates one download to one lost sale, is simplistic and inflates loss. In the absence of cogent evidence of the extent and impact of digital infringement, it seems difficult to describe technical measures as reflecting a fair balance.

(c) *Alternative means*

In *BT*, Parker J did not assess the comparative effectiveness and intrusiveness of alternative solutions to online enforcement. However, there are several obvious candidates which may constitute less intrusive means of reducing infringement. First, notice-and-takedown regimes already operate effectively, though they suffer from cross-border limitations and need greater harmonisation, as discussed in chapter 8. Second, automated enforcement systems such as YouTube's Content ID might provide greater accuracy and flexibility using fingerprinting technologies.[269] Third, more tailored technical measures — such as website blocking and de-indexing (discussed in chapter 7), data caps, connection shaping (limiting a subscriber's speed of access) or even sandboxing (restricting a subscriber to a whitelist of permitted news, entertainment and government websites) — could be just as effective as outright disconnection,

---

[266] Peter Hustinx, 'Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)' (22 February 2010) 19.

[267] Yu, above n 141, 1429–30.

[268] See, eg, Felix Oberholzer–Gee and Koleman Strumpf, 'File-Sharing and Copyright' in Josh Lerner and Scott Stern (eds), *Innovation Policy and the Economy* (2010) vol 10, 19 (attributing under 20 per cent of music sales declines to file-sharing).

[269] See Nathenson, above n 64 (ch 1), 938–44.

with significantly fewer spill-over effects. Fourth, technical measures could be reserved for those proved to be engaged in criminal infringements.[270]

Fifth, graduated response could be abandoned in favour of an 'expedited adjudication process', as the OECD recommended,[271] or fast track action against the primary wrongdoer in the First-Tier Tribunal, as discussed in chapter 4. Sixth, claimants could simply use existing remedies to claim damages from commercial infringers, distribution services, and bootleggers under existing procedures. Finally, as Patry observes, graduated response is 'all stick and no carrot'.[272] Regulators could reduce infringement by altering substantive copyright norms or encouraging claimants to make non-tortious modes of content acquisition more convenient, affordable and rewarding. The availability of these alternative mechanisms suggest that, in combination with a notification and identity disclosure regime, other measures have the potential to be at least as effective as technical measures with fewer harms. It is regrettable that courts and policymakers have neglected to consider these alternatives.

3.4 Compatibility with limitations

The *DEA* has been criticised as incompatible with safe harbours and general limitations applicable to ISPs under European law. Although some of these arguments are beyond the scope of this research,[273] this section will address two potential sources of incompatibility under the E-Commerce Directive: first, the mere conduit safe harbour; and second, monitoring obligations. It is suggested that both arguments were properly rejected in relation to the initial obligations in *BT*, but technical obligations warrant close examination if activated.

(a) *No mere conduit 'liability'*

There is a weak argument that the *DEA* is inconsistent with article 12 of the E-Commerce Directive. Article 12 protects intermediaries from liability arising *'for* the information transmitted', as might be the case under doctrines of secondary copyright liability. It does not protect from obligations to act 'in respect of' the information which arise for reasons unrelated to the transmission. Accordingly, in *BT* the *DEA* was held not to contravene article 12, which Parker

---

[270] See *Copyright Act* ss 107, 198, 296.

[271] OECD, *Public Policy*, above n 99 (ch 2), 155.

[272] Patry, above n 219, 12.

[273] These relate to the Data Protection Directive, Authorisation Directive, and cross-border services.

J held should be interpreted narrowly.[274] Any penalties were liabilities arising from the ISP's own misconduct under the Act rather than for transmitted information.[275] The Court of Appeal upheld this reasoning.[276]

While this distinction appears fine, it is correct for three reasons. First, on a proper understanding of the phrase 'not liable', a non-monetary obligation to forward notices is not relevantly a 'liability', even if it imposes an economic burden. It is analogous to obligations under *Norwich Pharmacal* orders, which are obligations arising only under the relevant court orders rather than *for* wrongdoing by the defendant or any other party.[277] The burden of notification is imposed independently of the information transmitted by the conduit, and therefore is not a liability 'for' that information. Similarly, obligations to contribute to the scheme's costs and any penalties for contraventions of the Act are 'essentially parasitic' obligations arising from the regulatory scheme and not from the information transmitted.

Second, the work done by article 12 relates to intermediaries' liability as primary and secondary infringers. However, it does not prohibit *any* obligation from being imposed on intermediaries simply by virtue of their being mere conduits. Third, the competing interpretation — that article 12 immunises intermediaries from *any* burden which would not have arisen without the transmission of information — is unsustainably broad. As Parker J reasoned, it would do violence to the language of article 12, which is conditioned on liability arising from the 'acts of transmission and of provision of access'.[278] Technical measures are also defensible, since article 12(3) expressly preserves the ability of courts and administrative authorities to require intermediaries to terminate or prevent infringements; technical measures may fall under this heading, but only if ordered by such public authorities.

(b) *No general monitoring duty*

Parker J also dismissed the suggestion that graduated response entailed a monitoring duty. Under the scheme, ISPs are 'essentially passive', reacting to notices and requests sent by qualifying copyright owners.[279] It is copyright owners who must monitor infringements and submit reports. ISPs are not obliged to inspect any information to determine whether an infringement has

---

[274] *BT*, [101] (Parker J).

[275] Ibid [107] (Parker J).

[276] *BT (CA)*, [53], [59] (Richards LJ) (Arden and Patten LJJ agreeing).

[277] See *BT*, [104] (Parker J) (drawing the same comparison).

[278] E-Commerce Directive art 12(2).

[279] *BT*, [115]–[116] (Parker J).

occurred — merely to forward and record the allegations. Accordingly, there was no breach of article 15. Barron criticises this analysis as 'artificial' because it ignores the reality that ISPs are acting as agents of claimants, who separately engage in general monitoring.[280] However, even if this analysis is correct, the result would be that ISPs' actions are attributed to claimants, and not the reverse, so Parker J's conclusion seems justified.

Conversely, requiring ISPs to disconnect or interfere with subscribers' connections might amount to a general monitoring duty if it required ISPs to satisfy themselves that the specified number of infringements had occurred. However, if technical measures were imposed by court order, it would be difficult to classify such duties as 'general' monitoring, since they would exist only in specific cases. Whether the new responsibilities of domain name registries amount to a general monitoring duty has not been determined, and would depend on the precise nature of policing required.

4 Conclusion

This analysis of intermediary copyright liability has identified two complementary approaches to enforcement: first, the incremental evolution of authorisation and joint liability doctrines, which apply fault-based standards to delimit the scope of monetary secondary liability; and second, the enactment of statutory regimes which mobilise ISPs in enforcing copyright against their subscribers and deterring infringement by individuals.

The first approach has many parallels with defamation liability. Intermediaries who are passive facilitators of third parties' infringements will rarely, if ever, face *prima facie* liability as authorisers or joint tortfeasors. Intermediaries who play more active roles — structuring their services towards infringing material, promoting infringing conduct or intentionally persuading others to infringe — can face liability, subject to the statutory safe-harbours identified previously. The second approach reflects growing consensus that problems of internet piracy are unlikely to be solved with liability rules alone. In this emerging tripartite enforcement structure, intermediaries' copyright liabilities are now shaped by a combination of common law and statutory secondary liability rules, regulatory obligations and injunctions. Although open to challenge for their economic costs, uncertain benefits and impact on fundamental rights, these statutory obligations forge a pragmatic, unprincipled compromise between strict and fault-based liability.

---

[280] Barron, above n 205, 332.

This chapter has argued that the initial obligations under the *DEA* are proportionate and, although their efficacy remains untested, may bring material benefits. These measures both mobilise and abandon intermediaries as loss avoiders:[281] the regulations require ISPs to act as claimants' agents, allowing copyright owners to pursue directly the individuals who engage in wrongdoing rather than gatekeepers who facilitate it. The *DEA* is an imperfect compromise. In particular, fairer cost-sharing is needed. It is unclear why ISPs should subsidise claimants' costs if they are not themselves tortfeasors and do not directly benefit from infringement. Nevertheless, the Act sufficiently respects the rule of law by requiring judicial determinations to be made at the crucial stage of disclosure and supplying opportunities for subscribers to contest wrongful allegations of infringement. However, like other commentators,[282] this research concludes that insufficient justifications have been shown for imposition of technical measures. The means reflected in the *DEA*'s technical obligations are unnecessary, ineffective and disproportionate.

While notification may impose no monetary liability or general monitoring duties, it still imposes considerable economic burdens on ISPs. Basic disagreement between member states over the legitimacy of graduated response only increases those costs, since digital infringement 'is an EU wide issue'.[283] The current arrangements pose a fundamental challenge to ISPs' business models, which are built on the assumption that they are conduits without responsibilities for *or arising from* the material transmitted by their customers. If this approach is extended to other intermediaries — particularly website operators, hosts and search engines — the result may be an explosion of notifications, higher costs to consumers and reduced innovation. However, long-term implications are difficult to predict; ironically, intermediaries may eventually become beneficiaries of stronger enforcement norms, particularly as their business models expand into content industries through bundling and video-on-demand services.[284]

Ultimately, even *sui generis* enforcement schemes may prove inadequate if not accompanied by other policies. As one senior executive of Apple Inc has observed:

> The solution to music piracy is not a technological one. No one can make the perfect safe to put things in. And it won't be a magic law that stops all piracy. In the end, the solution will be a behavioral one.[285]

---

[281] Cf Wu, above n 60 (ch 1), 344–5.

[282] Suzor and Fitzgerald, above n 139, 39.

[283] *BT*, [38] (Parker J).

[284] See, eg, Eduardo Porter, 'Keeping the Internet Neutral' (*The New York Times*, 9 May 2012) B1.

[285] Phil Shiller, Senior Vice President of Worldwide Product Marketing. See Alex Salkever, 'A Talk with iTunes' Conductor' (*Business Week*, 6 May 2003).

To similar effect, the government has concluded that infringement is unlikely to decline without legitimate services which 'allow consumers to access the type of content they want in a form and manner that best suits them and at a price they are willing to pay.'[286] Regulating consumer norms by coercion — whether in direct actions or by imposing secondary liability upon intermediaries — is inherently less effective than the 'versatile equilibrium of regulatory forces'[287] which presents consumers with new, non-tortious behavioural choices: education, convenient alternative content sources, and realignment of substantive copyright norms with consumer expectations are central to this process.

Like other parts of copyright law, developing these regulations requires striking a delicate balance between many competing interests in a way which inevitably will regulate competition between disseminators and incumbent industries.[288] The question of how this balance should be struck is 'a classic legislative task', rather than a judicial one.[289] Judicial decision-making is disproportionately slow, costly and forensically intensive relative to the value of the average internet infringement claim. Whatever policy is adopted, intermediaries will be its primary enforcers; care must be taken to ensure uniform statutory limits and mandatory assessments of internet users' rights. In circumstances where the benefits are uncertain and the social costs are likely to be high, prudence dictates that less intrusive alternatives be considered first.[290]

In chapters 6 and 7, we turn to consider two non-monetary equitable remedies which it is suggested can be effective and proportionate: duties to disclose the identity of primary wrongdoers; and duties to avoid facilitating access to tortious internet materials.

---

[286] BIS, *Consultation Document on Legislation to Address Illicit Peer-to-Peer (P2P) File-Sharing* (16 June 2009) 12.

[287] Michel Foucault, *About the Beginning of the Hermeneutics of the Self: Two Lectures at Dartmouth* (1993) 21 *Political Theory* 198, 204; Annemarie Bridy, 'Why Pirates (Still) Won't Behave' (2009) 40 *Rutgers Law Journal* 565, 611.

[288] See Wu, above n 60 (ch 1), 366.

[289] *BT*, [211] (Parker J).

[290] Yu, above n 141, 1402–3.

6
Disclosure

As chapters 4 and 5 have argued, there are many circumstances in which internet intermediaries are not liable to pay a monetary remedy for wrongdoing by their users. However, this is not the end of the inquiry. Chapters 6 and 7 examine two ancillary duties which are enforceable by injunction rather than damages: first, to disclose information about the identity of the primary wrongdoer; and second, not to facilitate access to tortious material. This chapter argues that an intermediary's obligation to disclose can be justified as the price which must be paid for immunity from monetary liability. Strong disclosure obligations complement that immunity by ensuring

the claimant can identify and seek redress from a tortfeasor who is *more* responsible for harm. Because disclosure indirectly regulates internet anonymity and speech, its boundaries must be carefully circumscribed. However, a robust, economical disclosure remedy is essential if claimants are to obtain redress from anonymous internet tortfeasors, and alleviates the pressure on intermediaries to act as loss-avoiders. An understanding of disclosure is therefore central to an analysis of their overall liability.

1 Introduction

Internet intermediaries frequently acquire information about tortious activity which is relevant to a claim against the primary wrongdoer. Such information can be relevant in two ways: first, it may reveal the identity of an anonymous user who is alleged to have committed a wrong; and second, it may supply evidence of the acts carried out by that user and the rights which the claimant says have been infringed. Obtaining access to this information is often essential for the claim to proceed, since without it the tortfeasor's identity may remain unknown. Disclosure therefore 'provides a remedy in circumstances where none would otherwise exist.'[1] However, disclosure is unusual because it is available without proof of wrongdoing by the disclosing party.

Faced with growing numbers of requests for information,[2] intermediaries are becoming gatekeepers not just of content but also of litigation. They control the missing pieces of the evidentiary jigsaw which claimants must assemble to bring a successful claim. This role has both procedural and substantive aspects: it is procedural in the sense that enforcement is by mandatory injunctions which enforce duties to the Court rather than duties to remedy wrongdoing. However, it is also described as a 'remedy',[3] a description which reflects four substantive attributes. First, applications for disclosure involve a preliminary consideration of the merits of the allegation against the third party wrongdoer ('the primary claim'). Second, an order for disclosure is final and compliance is mandatory on penalty of contempt. Third, giving disclosure may involve considerable expense. Finally, assessing a claim for disclosure is essentially a process of balancing the rights of claimants, internet users and intermediaries. Claimants desire access to justice and meaningful remedies against those who would defame them or infringe their copyrights online; internet users seek the freedom to receive and express information without compromising their

---

1 Charles Hollander, *Documentary Evidence* (10th ed, 2009) 93.

2 See, eg, Google Inc, 'Transparency Report — User Data Requests' (31 June 2011) <http://google.com/transparencyreport/data/> (showing 24.7 per cent increase in disclosure requests since January 2009).

3 See *British Steel Corporation v Granada Television Ltd* [1981] AC 1096, 1114 (Megarry VC) ('*British Steel*').

privacy. Intermediaries are caught in the middle: wishing neither to upset their customers nor incur primary liability to claimants, but seeking to minimise their operating costs and avoid acting in contempt of court.

The remedy of disclosure weighs these interests and places both lower and upper limits on the extent of intermediaries' cooperation. These boundaries are important because disclosure destroys anonymity. It does so by allowing claimants to aggregate fragments of an internet user's identity, piercing the curtain drawn between users on an intermediary's network and other internet users. Intermediaries and courts are natural gatekeepers of this process. This chapter argues that there is usually nothing inherently objectionable about de-anonymising internet communications for the purpose of identifying wrongdoers, provided the process is fair. Doing so upholds the rule of law by permitting claimants to complete their causes of action and so vindicate their rights. It is likely to increase the quality of expression online by deterring tortious conduct and holding users accountable for wrongdoing. However, requests for identity information must be rigorously examined. The primary claim must have realistic prospects of success. Requests which are unnecessary, disproportionately costly or likely to harm innocent users should be refused.

Despite widespread recognition that disclosure obligations may apply to intermediaries,[4] their nature and wider gatekeeping function has been largely unexamined by courts and scholars. Section 2 charts their expansion in cases involving offline intermediaries and argues that disclosure is best understood as comprising two distinct duties: to claimants and the Court. Section 3 draws on modern cases involving internet intermediaries to argue that non-monetary disclosure obligations are now well-established. Section 4 argues that the procedure is effective and compatible with European law, but makes several proposals designed to improve its proportionality and better protect third parties' rights.

2 The equitable protective jurisdiction

That the tortious activities of third parties can create duties to disclose their identities was accepted in *Norwich Pharmacal Co v Customs and Excise Commissioners*.[5] In this case, the defendant was a government department charged with administering taxes on goods imported into the United Kingdom. Pursuant to its statutory duties, the Customs kept records of each

---

[4] See, eg, Graham Smith, *Internet Law and Regulation* (4th ed, 2007) [6-003].

[5] [1974] AC 133 ('*Norwich Pharmacal*').

consignment's consignor, consignee, and description. The patentees became aware that third parties were importing their patented compound without permission but did not know who. They therefore sought disclosure of the names from the Customs. The House of Lords unanimously granted the application. Lord Reid identified in the authorities

> a very reasonable principle that if through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers.[6]

Lord Kilbrandon stated the duty in relational, rather than causal terms, requiring the intermediary to 'stand in some relation to' the owner of the goods,[7] which reflects the American formulation.[8] The Customs' physical control over the goods, knowledge of their nature, and statutory functions together established a relationship sufficient to impose an equitable duty of disclosure. Lord Morris emphasised that there must be a reasonably arguable case of primary wrongdoing, and that here any third parties identified in consignment documents could 'reasonably be assumed to be wrongdoers'.[9] In the Court of Appeal, the resulting obligation was described by Buckley LJ as an 'equitable duty', which comprised two related elements: not to part with infringing goods and to give all necessary information to the claimant.[10] The remedy for breach of either limb was an injunction, but no action for damages would lie against the defendant. In subsequent proceedings, the primary claim was tested and proved against the identified consignor, who was held to be a joint tortfeasor with the consignees.[11]

2.1 Historical development of the equitable jurisdiction

The disclosure principle has its basis in the equitable protective jurisdiction, pursuant to which a person could bring an action for a bill of discovery against a non-party, provided that person was not a 'mere witness'.[12] Until *Norwich Pharmacal*, the general rule was that no action for discovery lay against an innocent party unless an independent cause of action could be maintained against

---

6 Ibid 175 (Lord Reid).

7 Ibid 204 (Lord Kilbrandon).

8 Cf *Pressed Steel Car Co v Union Pacific Railway Co*, 240 F 135, 136 (DC, 1917) (Judge Learned Hand); *Post v Toledo, Cincinnati and St Louis Railroad Co*, 11 NE Rep 540, 547 (Ma SC, 1887).

9 *Norwich Pharmacal*, 179 (Lord Morris).

10 Ibid 145–6 (Buckley LJ).

11 See *Morton Norwich Products v Intercen* [1978] RPC 501.

12 *Interbrew SA v Financial Times Ltd* [2002] EMLR 24, 457, 460 (Sedley LJ) ('*Interbrew*').

that party.[13] This rule is best understood as a procedural anachronism deriving from the separate administration of equity and common law;[14] its main purpose[15] was to prevent disclosure from being ordered against a person who would ultimately be compellable to give evidence as a witness.[16] In this way, the mere witness rule simply *delayed* rather than excluded disclosure.[17]

By the late 19th century, offline intermediaries were routinely ordered to give over what information they knew unless 'absolute necessity' could be shown.[18] Almost any involvement in a wrong was sufficient to evade the mere witness rule, leading Hollander to conclude that it 'has, in essence, disappeared'.[19] Many were claims against the 19th century equivalents of ISPs — wharfingers, carriers or forwarding agents who transported or stored infringing goods on behalf of the primary tortfeasor and thereby 'facilitated' the wrongdoing.[20] In *Orr v Diaper*,[21] for example, the defendants were shippers who had been transporting cotton thread in coloured papers which imitated the claimants' distinctive packaging. Hall VC ordered disclosure.[22] Diaper's liability was limited: as a wrongdoer in equity but not a tortfeasor at law, he could be enjoined from passing on the counterfeit goods under the protective jurisdiction, but not liable to pay damages to the claimant. Other examples abound of carrier intermediaries being obliged to furnish information once mixed up with a wrongful transaction by acquiring knowledge. In *Upmann v Elkan*, a dock company came under a duty 'absolute and without qualification' to hold counterfeit goods and furnish upon the trade mark owner all relevant facts, once notified.[23] The reasoning was prescient: like modern cases, it requires purveyors of new technologies (in this case for transmission of goods) to police wrongdoing made possible by their services.

---

13 *Norwich Pharmacal*, 185 (Viscount Dilhorne). See, eg, *Plummer v May* (1750) 1 Ves Sen 426, 426; 27 ER 1121, 1122 (Lord Hardwicke LC).

14 See *Evidence Amendment Act 1851* (14 & 15 Vict c 99); *Common Law Procedure Act 1852* (Imp).

15 Doubtless the rule also served other purposes; it protected persons with an insufficient interest in the proceeding from being named as parties by providing grounds for a demurrer: John Mitford, *Mitford's Pleading* (4th ed, 1827) 191. It also restricted the collateral purpose of using bills of discovery to delay a parallel common law action: see *Norwich Pharmacal*, 192 (Lord Cross); *Hunt v Maniere* (1864) 34 Beav 157; 55 ER 594.

16 Charles Hollander, '*Norwich Pharmacal* Takes Wings' (2009) 28 *Civil Justice Quarterly* 458, 458.

17 *Norwich Pharmacal*, 174 (Lord Reid).

18 *Dixon v Enoch* (1872) LR 13 Eq 394, 400 (Wickens VC) (emphasis added).

19 Hollander, above n 16, 464.

20 *Norwich Pharmacal*, 139 (Lord Denning MR), 197 (Lord Cross).

21 (1876) LR 4 Ch D 92.

22 Ibid 95 (Hall VC); *Norwich Pharmacal*, 181 (Lord Morris).

23 See, eg, *Upmann v Elkan* (1871) LR 12 Eq 140, 145–6 (Lord Romilly MR); *Upmann v Forester* (1883) 24 Ch D 231, 235 (Chitty J). The Lord Chancellor remarked of intermediary immunity that 'I cannot conceive a doctrine more dangerous or mischievous … with respect to trademarks': ibid 132 (Lord Hatherley LC).

What the Court recognised in *Norwich Pharmacal* was that the mere witness rule was never intended to apply where there was no prospect of a trial without disclosure. Although Lord Kilbrandon criticised the rule as 'settled, rightly or wrongly',[24] it had no application where

> the whole basis of the application is that, until the defendant has disclosed what he knows, there can be no litigation in which he could give evidence.[25]

Thus, a person who facilitates the commission of the primary wrong and holds the crucial information is not a mere bystander or witness to the wrong. His involvement goes beyond spectatorship and places him an 'intermediate position' between witness and tortfeasor. It was this facilitating conduct — the getting 'mixed up in the tortious acts of others' — which Lord Reid sensibly said excludes cases like *Norwich Pharmacal* from the operation of the mere witness rule, to the extent it survives.

2.2 The nature of liability

Before considering the disclosure duties of internet intermediaries, it is necessary to understand that liability to disclose under the terms of a *Norwich Pharmacal* order is not the same as liability to pay damages or another monetary remedy. As Lord Woolf CJ pointed out in *Ashworth Hospital Authority v MGN Ltd*,[26] the jurisdiction applies to a person who, 'without incurring any personal liability, becomes involved in a wrongful act of another'. The order is thus not a remedy for wrongdoing by the disclosing party, but an exercise of the equitable protective jurisdiction by which claimants are guaranteed access to justice.

Cases variously describe this protective jurisdiction as 'an equitable duty'[27] not to facilitate infringement, a 'mere *quia timet* action' to prevent the primary wrong,[28] 'a duty to assist the person injured … by giving him any information which he is able to give',[29] and even 'a stand-alone remedy',[30] 'substantive relief',[31] and a 'substantive remedy of discovery'.[32] In the latter case, Megarry VC described the equitable jurisdiction as a separate cause of action whose sole relief was

---

[24] *Norwich Pharmacal*, 202–3.

[25] Ibid 203 (Lord Kilbrandon).

[26] [2002] 1 WLR 2033, 2039 ('*Ashworth*').

[27] *Norwich Pharmacal*, 145 (Buckley LJ).

[28] *One in a Million*, 920 (Aldous LJ) (passing off). See also *Microsoft Corporation v Ling* [2006] EWHC 1619 (Ch), [36] (HHJ Havery QC).

[29] *Ashworth*, 2039 (Lord Woolf CJ) (Lord Slynn agreeing). See also *British Steel*, 1104 (Megarry VC).

[30] *Shlaimoun v Mining Technologies International Inc* [2011] EWHC 3278 (QB), [24] (Coulson J).

[31] *Lockton Companies International v Persons Unknown* [2009] EWHC 3423 (QB), [4] (Eady J).

[32] *British Steel*, 1114 (Megarry VC).

disclosure, which is 'just as much an action for equitable relief as an action for specific performance or an injunction.'[33] This duty bears some similarities to the various species of secondary liability examined in previous chapters — because it derives from an independently-caused primary wrong — but it is conceptually distinct.

It is common to speak of a *Norwich Pharmacal* 'order' or a 'duty' of disclosure as if it were a unitary obligation. It is more accurate to describe disclosure as comprising two related duties. The originating equitable duty arises when a defendant first becomes mixed up in wrongdoing, to disclose what he knows about it. It is ancillary to the claimant's rights against the primary wrongdoer. Depending on the nature of the primary wrong, a duty not to part with infringing goods may also arise. The defendant may of course give disclosure voluntarily, or he can be ordered to do so by injunction. At this point a second set of obligations arise, which compel the defendant to act or face criminal liability as a contemnor, but do not provide any substitutive remedy for the defendant's prior failure to give disclosure. These obligations are owed to the Court — to comply with the injunction's terms — rather than to the claimant. Consistent with this view, disclosure remedies are not products of a mechanistic formula for relief but instead depend upon the exercise of judicial discretion.[34]

It follows from this that *Norwich Pharmacal* remedies do not themselves create liability to the claimant. Rather, such orders are properly understood as mandatory injunctions which simply crystallise the equitable obligation of disclosure into a new duty to the Court. This duty is superimposed upon the existing framework of relationships between an intermediary and third parties. It overrides any existing duties of confidentiality owed by the intermediary to its customers, and obliges cooperative measures 'which but for the order would be a gross breach of contract'.[35] It is, in short, a supervening obligation imposed by the court whose object is the preservation of the applicant's rights and thereby the proper administration of justice.

A disclosure order thus operates in a similar fashion to a freezing injunction,[36] which is routinely served on banks and other financial intermediaries, except that it is mandatory (requiring positive acts of disclosure) rather than prohibitory (preventing acts dissipating assets), and is generally made against the intermediary directly (rather than against the debtor himself

---

[33] Ibid (Megarry VC).

[34] *Norwich Pharmacal*, 176 (Lord Reid), 182 (Lord Morris), 190 (Viscount Dilhorne), 199 (Lord Cross), 206 (Lord Kilbrandon).

[35] *Customs and Excise Commissioners v Barclays Bank plc* [2007] 1 AC 181, 194 (Lord Bingham) (Lord Bingham) ('*Barclays Bank*').

[36] See *Mareva Compania Naviera SA v International Bulkcarriers SA* [1975] 2 Lloyd's Rep 509 ('*Mareva*'); *Civil Procedure Rules* r 25.1(1)(f).

and then notified to the intermediary). For financial intermediaries, 'receiving notice of such injunctions is, literally, an everyday event'.[37] However, the injunction does not create any new duty to the claimant — only a duty owed to the Court. As such, a freezing order is 'enforceable only by the court's power to punish those who break its orders' and not in an action for negligence.[38] It says to the defendant and any notified parties: comply or face liability as a contemnor.

Subject to these differences, a *Norwich Pharmacal* order operates analogously. Lord Bingham expressly made the comparison in *Barclays Bank*, placing disclosure orders into the same category of non-consensual orders that do not create duties of care but simply give effect to existing equitable duties. In *Ashworth*, Lord Woolf CJ accepted a similar analogy.[39] The liability which flows from breach of a *Norwich Pharmacal* order is therefore one arising under the Court's processes. This is unlike, for example, an injunction that requires the defendant to discontinue tortious activity, breach of which may sound not only in contempt but also in damages. However, because the liability of the defendant is strict, accidental breach by the addressee can still be sufficient — for example, because an internet intermediary accidentally deletes the relevant data, assists another party to breach the order,[40] or simply does not comply within a reasonable time and thereby frustrates its purpose.[41] Nevertheless, in all these cases, the claimant has no monetary remedy against the intermediary.[42]

2.3 Rationale

The primary purpose of disclosure is to enable the claimant to identify someone who has done him wrong. The Court orders disclosure in circumstances where, without it, he would not know whom to sue. Relatively few scholars have considered the theoretical justifications for this jurisdiction, which broadly fall into three categories: (1) preserving claimants' rights; (2) upholding the administration of justice; and (3) efficiency.

---

37 *Barclays Bank*, 194 (Lord Bingham); *Searose*, 895 (Robert Goff J).

38 *Barclays Bank*, 191 (Lord Bingham). See also ibid 221 (Lord Mance)

39 *Ashworth*, 2048 (Lord Woolf CJ) (Lord Slynn agreeing).

40 See *Attorney General v Times Newspapers Ltd* [1992] 1 AC 191.

41 See *Attorney General v Punch Ltd* [2003] 1 AC 1046; *Z Ltd v A-Z and AA-LL* [1982] QB 558, 578 (Eveleigh LJ).

42 Whether a breaching intermediary will face criminal liability is beyond the scope of this chapter, but see *Attorney General v Times Newspapers Ltd* [1992] 1 AC 191, 217 (Lord Oliver).

(a) *Preserving claimants' rights*

Without disclosure, ignorance of the wrongdoer's identity would be a fatal roadblock on the claimant's path to an effective remedy. Courts have long been mindful of the injustice that would result if claimants were left without recourse:

> In this case the plaintiffs do not know, and cannot discover, who the persons are who have invaded their rights … Their proceedings have come to a deadlock, and it would be a denial of justice if means could not be found in this court to assist the plaintiffs.[43]

As Lord Morris commented in *Norwich Pharmacal*, without disclosure primary infringers could act with impunity.[44] Disclosure thus 'enable[s] justice to be done.'[45] This explains why it does not depend on wrongdoing by the defendant: its purpose is to avoid injustice to the claimant by intervening to 'complete the cause of action'.[46] This also explains why the claimant is not required to commence proceedings: the information may be used to obtain redress by another means (such as negotiated settlement or lawful retaliation).

Disclosure is sometimes justified by reference to claimants' property rights. As Roskill LJ remarked in *Norwich Pharmacal*, disclosure was necessary because '[o]therwise rights accorded them under patents … are denied them'.[47] This is, of course, an incomplete explanation, since disclosure orders extend beyond primary wrongs involving property. These statements reflect the idea that by facilitating some interference with the claimant's rights, the defendant has incurred a new obligation to preserve the integrity of the claimant's secondary rights to a substitutive remedy. Disclosure protects those secondary rights by enabling them to be meaningfully exercised against the true wrongdoer.

(b) *Upholding the administration of justice*

The potential for injustice is a powerful reason for *Norwich Pharmacal* orders. However, claimants' rights are not dispositive of an application for relief. Various limitations and countervailing factors are considered, including proportionality, the fundamental rights of third parties, the confidentiality of data that are sought, statutory limitations upon disclosure,[48] and other

---

43 *Orr v Diaper* (1876) LR 4 Ch D 92, 96 (Hall VC); 25 WR 23.

44 *Norwich Pharmacal*, 179 (Lord Morris).

45 *British Steel*, 1132 (Templeman LJ).

46 *Interbrew*, 460 (Sedley LJ).

47 *Norwich Pharmacal*, 147 (Roskill LJ). See also *British Steel*, 1141 (Watkins LJ); *R (on the application of Revenue and Customs Commissioners) v W* [2008] EWHC 2780 (Admin), [38]–[39] (Ouseley J).

48 See, eg, *Contempt of Court Act 1981* (UK) s 10.

considerations of public policy. Its essential purpose is 'to do justice'.[49] Doing justice to claimants therefore cannot be a complete explanation. A second category of justifications frames the remedy in terms which accommodate this delicate balancing of public and private interests: disclosure is said to be an incident of the 'duty of the court to assist with the administration of justice'.[50] This explains why equity protects the mere witness from disclosure suits even though they might possess relevant information: examination as a regular witness is simply more proportionate to their degree of involvement and the legitimate aim of seeking redress against the primary wrongdoer.[51] Such third parties hold a legitimate expectation that they will not be intruded upon and swept up in litigation. When given, disclosure upholds the rule of law by ensuring claimants can bring their causes before competent tribunals rather than relying upon self-help or forbearance.

A related justification reflects the assumption that a defendant who enables or causes wrongdoing, however innocently, is more culpable than a party who had no causal connection to wrongdoing. As Lord Reid put it in *Norwich Pharmacal*, 'justice requires that he should co-operate in righting the wrong if he unwittingly facilitated its perpetration.'[52] This 'duty to assist'[53] — sometimes described using the language of unconscionability[54] — is difficult to sustain, since the obligation to disclose arises regardless of whether the defendant's facilitation is an actionable wrong. Assistance without more is not tortious,[55] but it is often sufficient for disclosure. Disclosure is in reality a no-fault response to conduct causing harm, even if that conduct otherwise creates no liability.

(c) *Efficiency*

Finally, *Norwich Pharmacal* orders promote efficiency by compelling parties who deal with rogues and other 'dishonest correspondents' to internalise the cost of identifying those whose wrongs they enable. Disclosure imposes a relatively small search cost on the disclosing party compared to the large cost faced by a claimant who is forced to wear his losses or acquire the information by

---

[49] *Viagogo (SC)*, 3338 (Lord Kerr JSC).

[50] *Colonial Government v Tatham* (1902) 23 Natal LR 153, 158 (Beaumont AJ); *Harrington v Polytechnic of North London* [1984] 1 WLR 1293, 1299 (Sir John Donaldson MR); *Mitsui*, [24].

[51] See *Mersey Care NHS Trust v Ackroyd* [2006] EMLR 12, 318 (Tugendhat J); *Ashworth*, 2051 (Lord Woolf CJ) (Lord Slynn agreeing).

[52] *Norwich Pharmacal*, 175 (Lord Reid).

[53] *Bankers Trust Co v Shapira* [1980] 1 WLR 1274, 1282 (Lord Denning MR).

[54] *Jade Engineering (Coventry) Ltd v Antiference Window Systems Ltd* [1996] FSR 461, 466 (Jacob J) ('*Jade Engineering*').

[55] See above chapter 3, § 1.3(b)(iii).

alternate means. This reflects the reasonable assumption that a person mixed up in anonymous wrongdoing is a lesser cost avoider than its victim, since the former already possesses information necessary for the victim to seek redress. In resisting disclosure, defendants tend to exaggerate the costs of compliance and urge the Court to refuse relief because it would 'cause manifest inconvenience to the citizens of this country whose only fault is that they happen to have some information that the plaintiff wants'.[56]

Courts have been largely unreceptive to these complaints. For example, Lord Kilbrandon in *Norwich Pharmacal* regarded the cost to the defendants as small compared to the benefits flowing to the claimant:

> the defendants will not be the losers, except in so far as *they may have been put to a little clerical trouble.* … [I]n *total disregard of … loss of time and money*, [they must] attend the court … to assist a private citizen to justify a claim in law. The policy of the administration of justice demands this service …[57]

This passage contrasts starkly with the conclusion of Buckley LJ in the Court of Appeal, who commented that the Commissioners were 'under no obligation to police the plaintiffs' immunity from infringement'.[58] While this is undoubtedly true, Lord Kilbrandon concluded that defendants should nevertheless 'assist' such policing where their enforcement costs are lower.

2.4 Expansion of the modern remedy

Since *Norwich Pharmacal*, the scope of equitable disclosure has grown dramatically. As Lord Woolf CJ observed in *Ashworth*:

> New situations are inevitably going to arise where it will be appropriate for the jurisdiction to be exercised where it has not been exercised previously. The limits which applied to its use in its infancy should not be allowed to stultify its use now that it has become a valuable and mature remedy …[59]

The relaxation of those limits demonstrates the flexibility of the modern remedy and its 'adaptation to new circumstances',[60] including the activities of internet intermediaries. It is no

---

[56] *Norwich Pharmacal*, 165 (Peter Oliver QC, in argument).

[57] Ibid 203 (Lord Kilbrandon).

[58] Ibid 142 (Buckley LJ).

[59] *Ashworth*, 2049 (Lord Woolf CJ) (Lord Slynn and Lord Browne-Wilkinson agreeing).

[60] *Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] EWHC 625 (Ch), [20] (Lightman J) ('*Mitsui*').

overstatement to describe these changes as 'striking'[61] or a 'revolution'.[62] Four aspects warrant comment.

(a) *Wrongdoing*

First, the standard to which the primary wrong must be proved has progressively slackened. *Norwich Pharmacal* was a case in which the third parties 'whose names are known to the commissioners *are wrongdoers*',[63] or could 'reasonably be assumed to be wrongdoers'. Forty years later, the threshold has been reduced to an 'arguable case' of wrongdoing.[64] Some authorities even suggest that disclosure is available without any primary wrong, to enable the claimant to determine whether a tort has in fact occurred,[65] or to identify persons whose wrongdoing is only speculative. In *Arab Satellite*, for example, the trial judge ordered disclosure of any third party 'who was or may have been involved in any way' in trespassing upon the claimant's satellite transponders, provided that it was possible for the applicant to 'sort the sheep from the goats'.[66] Similar logic could support an order being made to disclose subscriber IP addresses where it is uncertain which individual was responsible for an infringement. In such a case, like *Arab Satellite*, the pool of possible tortfeasors is likely to be small, making it possible to eliminate innocent parties.

Although the jurisdiction has its basis in the equitable bill of discovery, its scope clearly encompasses any 'tort, a breach of contract or other civil or criminal wrong',[67] including defamation and copyright infringement.[68] There seems no reason in principle to preclude any wrong from founding an action for disclosure.

---

61 Hollander, above n 19, 466.

62 Paul Cox, 'Evolution or Revolution? *Norwich Pharmacal Orders over the Last 20 Years*' (2004) 172 *Trademark World* 40, 40.

63 *Norwich Pharmacal*, 178 (Lord Morris) (emphasis added).

64 *R (on the application of Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2009] 1 WLR 2579, 2607 (Thomas LJ) ('*Mohamed*').

65 See, eg, *P v T Ltd* [1997] 1 WLR 1309 ('*P v T*') (though the order was in reality preliminary disclosure for the purpose of evaluating a potential claim against an identified tortfeasor).

66 *Arab Satellite Communications Organisation v Al Faqih* [2008] EWHC 2568 (QB) [25].

67 *Ashworth*, 2035 (Lord Slynn) (breach of contract). See also *Interbrew*, 457 (Sedley LJ).

68 See *P v T* (defamation); *RCA Corporation v Reddingtons Rare Records* [1974] 1 WLR 1445, 1446–7 (Goff J) (copyright).

(b) *Facilitation*

Second, concepts of involvement and facilitation have expanded. Lord Cross and Lord Kilbrandon originally described the required nexus as a 'relation'.[69] In *Ashworth*, Lord Woolf CJ stated that it is not a 'stringent requirement',[70] but the defendant must have 'participated' or been 'involved' in the wrongdoing,[71] of which innocent publication of wrongfully disclosed information was 'emphatic' evidence. Lord Morris required the defendant to be 'actually involved (or actively concerned)'[72] in the wrongdoing. Other authorities prefer to describe the defendant as being 'mixed up in' even if not 'causative of the wrongdoing'.[73] Beyond empty synonyms it is difficult to find any clear statement of principle that establishes the necessary *degree* of involvement.

The threshold does not appear to be high. The defendant's actions need not have been the legal cause of wrongdoing — Thomas LJ considered this conclusion 'plainly correct' in *Mohamed*.[74] Indirect facilitation is sufficient. Contrary to Lord Romilly MR in *Upmann v Elkan*, knowledge is now unnecessary: the defendant can be 'innocent and in ignorance of the wrongdoing' but still under a duty to disclose.[75] However, knowledge may suggest a degree of participation or involvement.[76] It is suggested that the authorities may be distilled as follows: any type of assistance — that is, any necessary cause of the acts constituting the wrong — will be enough, however minor and regardless of the mental state with which it is given, provided that in so giving it the defendant is not a mere witness.

(c) *Necessity*

Third, disclosure need no longer be strictly 'necessary' for taking action against the primary wrongdoer.[77] Traditionally, the information must have supplied the vital 'missing piece of the jigsaw'[78] and the defendant must be its only practicable source, consistent with the view of disclosure as a 'remedy of last resort'.[79] More recent cases have preferred a looser criterion: the

---

69 *Norwich Pharmacal*, 188 (Lord Cross).

70 *Ashworth*, [35] (Lord Woolf CJ) (Lord Slynn agreeing).

71 *Ashworth*, 2041 (Lord Woolf CJ) (Lord Slynn agreeing). This reflects the preferred formulation of Viscount Dilhorne in *Norwich Pharmacal*, 188.

72 *Norwich Pharmacal*, 178 (Lord Morris).

73 *Aamer v The Secretary of State for Foreign and Commonwealth Affairs* [2009] EWHC 3316 (Admin), [43].

74 *Mohamed*, [70].

75 *Ashworth*, [30] (Lord Woolf CJ).

76 *Mohamed*, [72]. Cf *Ricci v Chow* [1987] 1 WLR 1658, 1665 (Parker LJ), 1668 (Kerr LJ).

77 *Ashworth*, [57] (Lord Woolf CJ) (Lord Slynn agreeing).

78 *Mitsui*, [24] (Lightman J).

79 *Nikitin v Richards Butler LLP* [2007] EWHC 173 (QB), [24] (Langley J) ('*Nikitin*').

information must be necessary only in the sense that, in all the circumstances, the balance of convenience favours disclosure.[80] This is sensible, since otherwise disclosure might never strictly be *necessary* where multiple third parties are in possession of the same information (as is common where internet intermediaries are involved at multiple layers).[81] Consistent with this flexible approach, courts no longer insist upon the applicant intending to commence proceedings against the primary wrongdoer.[82] It is sufficient that that the applicant intends to take some legitimate action or have a 'legitimate reason' for wanting the information.[83] Importantly, this might be a foreign proceeding,[84] such as will frequently arise where cross-border wrongs are perpetrated online.

(d) *Proportionality*

Fourth, limitations upon disclosure have been articulated with greater flexibility. Traditionally, once wrongdoing, facilitation and necessity were shown, disclosure ordinarily followed unless the defendant could point to some consideration of public policy or other legitimate interest to defeat the claim.[85] That the information being sought is confidential or private is not necessarily a bar to disclosure. In *Norwich Pharmacal*, Lord Reid thought that wrongdoers should not be able to hide behind the confidentiality of customs data:

> If we could be sure that those whose names are sought are all tortfeasors, they do not deserve any protection.[86]

Similarly, data protection rights impose few limits of substance. In *Parkinson v Hawthorne*, the Court broadly construed s 35 of the *Data Protection Act*, which exempts disclosure necessary 'for the purpose of, or in connection with, any legal proceedings' or for 'establishing, exercising or defending legal rights.'[87] Patten J held that the provision 'removes any difficulty' and ordered disclosure of a judgment debtor's address from a land register.

---

80 *Campaign against Arms Trade v BAE Systems plc* [2007] EWHC 330 (QB), [15]–[20] (King J) ('*BAE*').

81 Cf *BMG Canada Inc v John Doe* (2005) 252 DLR (4th) 342, [35] ('*BMG Canada*'), where Sexton JA would have refused disclosure against an ISP if another intermediary was able to supply the same information.

82 See, eg, *CHC Software Care Ltd v Hopkins & Wood* [1993] FSR 241.

83 *Jade Engineering*, 466 (Jacob J). See, eg, *British Steel*, 1132 (Templeman LJ), 1127 (Lord Denning MR); *P v T* [1997] 1 WLR 1309, 1318–19 (Scott VC)

84 *Jade Engineering*, 466–7 (Jacob J). See also *R v W*, [38]–[39] (Ouseley J).

85 *Norwich Pharmacal*, 175 (Lord Reid), 182 (Lord Morris).

86 Ibid 176 (Lord Reid).

87 [2009] 1 WLR 1665, 1669 (Patten J).

As an equitable remedy, *Norwich Pharmacal* relief remains discretionary. Consistent with the overriding objective,[88] disclosure must be 'in the interests of justice'. This has been reinterpreted as a requirement of proportionality.[89] In short, the Court will consider whether the difficulty and expense involved in giving disclosure or breaching a parallel duty (of confidence, for example) is justified by a countervailing interest in disclosure. This may be because of the urgency of the information, its benefit to the claimant or the public, the unavailability of reasonably viable alternatives, the gravity of the primary wrong or the seriousness of the consequences if disclosure is not given.[90] Lord Bingham explained the preferred approach in *Equatorial Guinea v Royal Bank of Scotland International* as one which asks whether disclosure is reasonable having regard to the existence of other 'straightforward and available means of finding out' the wrongdoer's identity.[91] Since *Equatorial Guinea* and *Ashworth*, it seems doubtful whether the remedy is truly 'exceptional' and not simply a response to wrongdoing by an unknown party.[92] The focus is on whether disclosure is, in all the circumstances, a proportionate response to the defendant's participation in that wrongdoing and the claimant's other remedies.

3 Application to internet intermediaries

3.1 Platforms

Where a website or other platform facilitates wrongdoing, disclosure will normally be ordered against an operator who possesses information concerning the wrongdoer, unless the cost or other negative consequences of doing so are disproportionate to the loss suffered by the claimant. The cases may be divided into two main categories. In the first, the defendant administers a discussion forum, weblog or other application-layer service to which allegedly tortious information is posted by an anonymous party. The primary wrong lies in the publication or disclosure of the information, as the case may be, and the claimant seeks to learn the author's identity. In the second category, an online marketplace or payment intermediary facilitates tortious activities, such as trespasses or breaches of contract, by third parties in the real world. There the transmittal is necessary but antecedent to the tort, and the claimant seeks to know who took part in it. For

---

88 *Civil Procedure Rules* r 1.1(1).

89 See *Ricci v Chow* [1987] 1 WLR 1658.

90 See, eg, *Mohamed*, 2633 (Thomas LJ).

91 [2006] UKPC 7, [16] (Lord Bingham).

92 See Hollander, above n 1, [5-14], 108–9. Cf *Nikitin*, [30] (Langley J).

disclosure to be useful, the platform must retain some information which points towards the primary wrongdoer.[93]

In general, the principles applied in disclosure cases involving internet defendants are identical to those applied offline. However, particular factual considerations arise — in particular the privacy interests of internet users — which are relevant to the exercise of the Court's discretion. Several guiding criteria were set out in *Totalise plc v The Motley Fool Ltd*, where disclosure was ordered against the operator of a discussion forum in which a malicious campaign of abuse was conducted against the claimants by an anonymous user.[94] This approach was later adapted in *Rugby Football Union v Viagogo Ltd*[95] to apply a two-stage test based on necessity and proportionality. The authorities now suggest that whether users' or claimants' rights should prevail in a given case depends on several factors.[96]

(a) *Gravity of primary wrongdoing*

First, the Court will consider the nature and gravity of the tort alleged. Publication to a 'vast' or worldwide audience of 'plainly' tortious material will favour disclosure;[97] trivially tortious material will not. An example can be seen in *Sheffield Wednesday Football Club Ltd v Hargreaves*,[98] where messages had been posted pseudonymously to a discussion forum for fans of the Sheffield football club by forum users who were unhappy with the club's management. The claimants considered these messages defamatory and sought disclosure of the email addresses of 11 forum members. Although several messages contained arguably false and defamatory statements, they were mere 'saloon-bar moanings' with a 'smidgeon of personal abuse'[99] and only trivially defamatory. The Court exercised its discretion to refuse disclosure of their authors because to do so 'would be disproportionate and unjustifiably intrusive.'[100] HHJ Parkes QC ordered disclosure only in respect of the more serious postings alleging dishonesty or greed — there the claimants' rights to vindicate their reputations outweighed the privacy interests of users.

---

93 This is frequently the case for the reasons explained in §3.6.

94 [2001] EMLR 29; appeal allowed as to costs in [2002] 1 WLR 1233 ('*Totalise*').

95 [2011] EWCA Civ 1585 ('*Viagogo (CA)*'); aff'd *Rugby Football Union v Consolidated Services Ltd (formerly Viagogo Ltd) (in liq)* [2012] 1 WLR 3333 ('*Viagogo (SC)*').

96 Doubtless there are others, such as the protection of journalistic sources: see *Viagogo (SC)*, 3339 (Lord Kerr JSC).

97 *Totalise*, [26] (Owen J). Although unclear, this seems to involve objectively assessing whether a reasonable website operator ought to have known that the material was tortious.

98 [2007] EWHC 2375 (QB) ('*Sheffield*').

99 Ibid [18] (HHJ Parkes QC). Arguably, therefore, the postings were not defamatory at all, in the sense that they would not be understood to convey a defamatory meaning.

100 Ibid [17] (HHJ Parkes QC).

In requiring a threshold of seriousness before disclosure will be ordered, the Court excluded wrongs which, although arguable, are insubstantial or trivial. This litigation filter indirectly protects the interests of website users by preventing them from being exposed to the cost and inconvenience of defending an action which is unlikely to serve any legitimate purpose. To this extent, the filter goes beyond the 'arguable wrong' requirement; it both complements and pre-empts the Court's power to grant summary dismissal or strike out a claim as an abuse of process. The filter creates an additional threshold to justify the perceived inconvenience of depriving users of their anonymity without notice. Conversely, if disclosure would deter similar wrongdoing by others, this favours relief.[101]

(b) *Strength of the primary claim*

The second factor is the applicant's likelihood of success in the primary action; a weak or speculative claim is less likely to support disclosure. In *Clift v Clarke*,[102] Sharp J refused an order against the editor of a news website on which offensive comments were posted about the claimant by pseudonymous users. Referring to *Sheffield*, Sharp J held that disclosure of the commenters' identities would be disproportionate having regard to the weakness of the primary claims in defamation; from their nature and context, the comments were unlikely to carry defamatory meanings and a defence of honest comment was available.[103] In reality, the postings were merely 'pub talk': abusive but light-hearted statements that were unlikely to be taken seriously by reasonable readers.[104] Accordingly, disclosure should have failed by reason of there being no primary wrong at all. Like *Sheffield*'s 'substantiality', this criterion functions as a litigation filter which shields website users from disclosure in support of actions which are clearly doomed to fail.

(c) *Reasonable expectations of privacy*

A third factor is whether, in the circumstances, platform users have a reasonable expectation that their personal data will not be disclosed. Although such disclosure is permitted under *DPA* s 35(1),[105] the fifth and sixth Data Protection Principles still require the Court to be satisfied that disclosure is warranted having regard to the rights and freedoms or legitimate interests of the

---

[101] *Viagogo (SC)*, 3339 (Lord Kerr JSC); *Ashworth*, [66] (Lord Woolf CJ).

[102] [2011] EWHC 1164 (QB) ('*Clift*').

[103] Ibid [40]–[42] (Sharp J).

[104] Ibid [35]–[36] (Sharp J). Cf *Thornton v Telegraph Media Ltd* [2010] EWHC 1414 (QB).

[105] *Totalise* [2001] EMLR 29, [21] (Owen J).

data subject.[106] For this purpose, the Court must give 'close consideration' to whether disclosure would unjustifiably invade the user's *Convention* and *Charter* rights to respect for his private life and personal data.[107] This inquiry has two distinct stages: first, asking whether the user holds a reasonable expectation of privacy in respect of the data; and second, asking whether, after balancing that expectation against the public interest in disclosure, the scales are tipped in favour of the claimant.

The starting point in answering the first of these questions is normally the website's terms of service and other policies. In *Sheffield*, the forum's policies prohibited defamatory and abusive language, and offered no guarantees of secrecy to users. In *Clift*, the website's terms prohibited the posting of defamatory or abusive material but safeguarded commenters' personal information from disclosure, except as required by law. The courts held that in the latter case, users enjoyed a reasonable expectation of privacy, but in the former case they did not. The conclusion in *Clift* is open to question because the postings were probably abusive and therefore violated the policy as stated. The decision is therefore better treated as resting on the basis that there was no arguable wrongdoing.

In practice, once arguable wrongdoing is established, courts very rarely prioritise the interests of potential tortfeasors. In *Totalise*, Owen J concluded that

> the respect for and protection of the privacy of those who chose to air their views in the most public of fora must take second place to the obligation imposed upon those who become involved in the tortious acts of others to assist the party injured by those acts.[108]

Similar reasoning was applied in *Viagogo* to order disclosure against an online marketplace which provided a secondary market for sporting tickets. The defendant had advertised tickets to the claimant's rugby matches at Twickenham, which were being resold by third parties — often at substantial premiums over their face value — contrary to the original terms of sale. The defendant generally did not sell the tickets itself but merely facilitated transactions between third parties, whose names and addresses it retained. The claimant sought disclosure of this information for the purpose of bringing proceedings against sellers for breach of the ticket conditions, conversion of the paper ticket, and jointly committing trespass with buyers who falsely gained admission to matches using a resold ticket.

---

[106] *Totalise*, 1239 (Aldous LJ).

[107] *Viagogo (SC)*, 3347 (Lord Kerr JSC). See *Charter* art 8; Data Protection Directive art 7; *Bonnier*, [59]–[60].

[108] *Totalise* [2001] EMLR 29, [26] (Owen J).

The trial judge, Court of Appeal and Supreme Court all agreed that sellers and buyers of resold tickets did not have a reasonable expectation of privacy. Viagogo's terms of use expressly contemplated disclosure under compulsory legal processes and, in any case, arguable wrongdoers cannot wear the mantle of privacy to conceal their arguable wrongs:

> There can be no reasonable expectation of privacy in respect of data which reveal such arguable wrongs and Viagogo's own conditions of business point out to their customers that … their personal data will be passed on to others.[109]

From an analysis of the contractual matrix and evidence of unauthorised ticket sales, Longmore LJ concluded that there were at least arguable claims of breach of contract and trespasses for which sellers may be held jointly liable.[110] Accordingly, Viagogo's customers could not invoke privacy to conceal these allegations of misconduct. Obtaining injunctive relief against ticket sellers was a legitimate purpose of disclosure notwithstanding that any monetary relief may be insubstantial or that claims for damages may ultimately fail.[111] The Supreme Court took an even broader view of the claimant's purpose, which should not be considered 'in a hermetically sealed compartment'; it was enough simply to seek disclosure with a view to deterring others from buying or selling tickets in the future.[112]

Both appellate courts rejected Viagogo's submission that s 35(1) must be construed to apply only where disclosure is 'strictly necessary' and proportionate to the purpose of protecting the claimant's rights, as explained by the CJEU.[113] Either standard would be satisfied where the disclosure order only affects the personal information of arguable wrongdoers. If all users of Viagogo who transacted in tickets to Union matches presumptively breached the applicant's conditions by advertising or purchasing resold tickets, there were no 'innocent' users whose expectations of privacy might be infringed.[114] At most it could be said that they were ignorant that what they were doing was tortious, which was irrelevant. Moreover, there was no particular sensitivity or confidentiality in ticket sales data (unlike, perhaps, downloaders of pornographic films). Accordingly, disclosure was in the interests of justice. For similar reasons, the Supreme Court rejected an argument that disclosure would be contrary to users' rights under article 8 of

---

[109] *Viagogo (CA)*, [28] (Longmore LJ).

[110] Ibid [19]–[20] (Longmore LJ). See also *Viagogo* [2011] EWHC 764 (QB), [45] [54], [56] (Tugendhat J).

[111] *Viagogo (CA)*, [24] (Longmore LJ). This reasoning side-steps the requirement of *Clift* and *Sheffield* that the primary wrong meet a threshold of substantiality.

[112] *Viagogo (SC)*, [36]–[37], [40] (Lord Kerr JSC).

[113] See Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy* [2008] ECR 1-9831, [52]–[56]; Case C-92/09, *Schecke GbR v Land Hessen* [2011] 1 Info LR 366, [86].

[114] *Viagogo (SC)*, [43], [45] (Lord Kerr JSC).

the *Charter*. In upholding the order for disclosure, the Supreme Court was clearly motivated by its impression of the 'entirely worthy' motives of the claimant in seeking to promote Rugby Union and reduce the price of tickets, efforts which were 'frustrated' by the defendant's anonymous marketplace, which enabled 'ticket touts' to act 'in stark breach' of its terms and policies.[115]

In *BT*, the Court of Appeal endorsed an equally broad reading of s 35. Although the *DEA* was primarily designed to educate infringers rather than result in legal claims being brought against them, disclosure and processing of repeat infringers' identities still fell within the exemption in article 8(2)(e) of the Data Protection Directive (corresponding to s 35 of the *DPA*) since it was 'plainly necessary' for establishing, exercising or defending claimants' legal rights.[116] As discussed in section 4.3(e), if this reasoning becomes orthodoxy, privacy will offer illusory protection from disclosure.

(d) *Realistic alternatives to disclosure*

Fourth, disclosure is more likely to be granted if there are no realistic alternatives open to the claimant to protect its rights. In *Viagogo*, the claimant could theoretically have made trap purchases, inquired of its distributors and club sponsors, or conducted spot checks at stadium entrances, but these alternatives were either excessively costly or unlikely to be met with cooperation from clubs (who risked paying contractual penalties) or patrons who were refused admission. In this regard, whether disclosure was 'necessary' was treated as a question of whether, absent disclosure, there existed any 'straightforward or available means of finding out the information'[117] — a lower threshold than *Norwich Pharmacal* or even *Mohamed*.[118] Disclosure was necessary because there was no other way — short of fundamentally altering its business operations — for the Union to identify or stop the sellers responsible.[119] While the lack of alternatives will often favour a finding of proportionality, it is not inevitable; in 'limited instances', data subjects' rights may be so strong as to displace the claimant's interest in disclosure.[120] Nevertheless, *Viagogo* clearly demonstrates that intermediaries can be brought within the

---

[115] Ibid [2], [36], [45] (Lord Kerr JSC).

[116] *BT*, [76]–[77] (Richards LJ).

[117] *Viagogo*, [63], [70] (Tugendhat J).

[118] Cf *Mobilisa Inc v Doe 1*, 170 P 3d 712, 715 (Ariz Ct App, 2007) ('*Mobilisa*').

[119] *Viagogo (CA)*, [26] (Longmore LJ).

[120] There is, accordingly, no presumption in favour of proportionality: *Viagogo (SC)*, [46] (Lord Kerr JSC).

protective jurisdiction even where disclosure is not 'strictly necessary' because alternative (but impractical) sources of information about the primary wrongdoers exist.

(e) *Cost and impact of disclosure*

Fifth, the Court will evaluate the cost and impact of disclosure to the website operator against the importance of the information to the claimant. An example can be seen in *Microsoft Corporation v Plato Technology Ltd*,[121] where *Norwich Pharmacal* relief was refused against a distributor who innocently resold counterfeit software because the orders against it would be ruinous to its business.[122] Compared to the small scale of infringement, the impact on the defendant was oppressive and disproportionate. By contrast, in *Viagogo* the Court rejected the defendant's submission that disclosure would deter individuals from using its marketplace for legitimate sales. Greater harm was being caused to the claimant by unauthorised ticket sales. This is unlike *Plato*, where only a small number of counterfeit copies were sold and there was no evidence of ongoing harm.

(f) *Conduct of platform operator*

Sixth, the Court will examine the conduct of the platform operator. If the defendant 'supported' the tort or acted to 'obstruct justice', then disclosure is *prima facie* appropriate. If, however, the defendant acted neutrally, the claimant bears the onus of establishing that a refusal to disclose was unjustified.[123] In most cases, this will not be a difficult hurdle, as two cases involving neutral intermediaries demonstrate. First, in *G v Wikimedia Inc*,[124] an unknown third party had edited a page on Wikipedia to include confidential information about the applicant and her child. The claimant sought the author's IP address. Wikipedia refused, citing its policy of not releasing personal information without a court order, but did not oppose the claimant's application, which the Court granted without further elaboration.

Second, in *Bacon v Automattic Inc*,[125] similar orders were made against Wikipedia, a weblog platform and an American news website. Each defendant had innocently disseminated anonymous

---

[121] [1999] FSR 834 ('*Plato*').

[122] Ibid 846 (HHJ Steinfeld QC).

[123] *Totalise*, 1241 (Aldous LJ).

[124] *G v Wikimedia Foundation Inc* [2010] EMLR 14, 364 ('*Wikimedia*'). The material was later removed by a Wikipedia volunteer.

[125] [2011] EWHC 1072 (QB).

defamatory postings and refused to disclose voluntarily. Although they were not suggested to be liable, Tugendhat J again granted requests for service.[126] These intermediaries' immunity from monetary liability did not exclude their non-monetary disclosure obligations.

3.2 Hosts

Orders against hosts are less common, and only a handful of reported cases exist. Nevertheless, it is clear that proprietors of servers may owe duties to disclose information stored on them. Such information commonly takes the form of email messages, access logs, routing information and other technical data which can be used to identify a tortfeasor. Hosts facilitate primary wrongdoing in similar ways to website operators: typically by storing or routing data that are essential to wrongdoing. For example, Blogger 'plainly facilitates' the storage and publication of defamatory postings.[127]

Participation does not always require tortious content to be published on the public internet; it may be transmitted or stored privately. In *Takenaka (UK) Ltd v Frankl*, the claimants obtained information about a defamatory email from a number of hosts, including Microsoft's Hotmail and Compuserve. That information enabled the claimants to trace the origin of the email to the defendant's computer in Turkey.[128] In another case concerning emails, the respondent had received a message containing wrongfully obtained confidential information. It notified the claimant, who obtained disclosure of the sender so it could identify the source of the leak.[129] More recently, in *Lockton Companies International v Google Inc*[130] the claimants identified the authors of tortious emails which had been sent anonymously using Google's Gmail mail-server. Although the server was operated in the United States, Eady J held that disclosure was appropriate on well-established principles.[131]

3.3 ISPs

Disclosure orders are routinely made against English ISPs that transmit data on behalf of subscribers engaged in tortious activity. Their purpose is usually to enable a claimant to discover

---

[126] Ibid [16], [53] (Tugendhat J).

[127] *Tamiz (CA)*, [25] (Richards LJ).

[128] *Takenaka (UK) Ltd v Frankl* [2001] EWCA Civ 348, [28] (Mance LJ), [36] (Ward LJ).

[129] *BAE*, [73], [86], [95] (King J).

[130] [2009] EWHC 3423 (QB).

[131] Although a foreign defendant may not be joined solely for the purpose of disclosure, Eady J classified *Norwich Pharmacal* disclosure as the 'substantive relief' sought in the action: ibid [4]–[5].

the accountholder associated with an IP address which is suspected of being connected with wrongdoing at a particular time. Actions tend to be commenced in bulk and seek to identify many thousands of IP addresses, frequently but not always for the purpose of asserting copyright infringement. This often involves uncovering the personal information of subscribers, such as browsing history and details of accessed files. These attributes — scale, untested claims and private data — create considerable potential for abuse. Nevertheless, in most cases disclosure will be an uncontroversial exercise of the equitable jurisdiction, and the courts have struggled to article meaningful limits on the use of disclosed subscriber data.

(a) *Threshold of facilitation*

English courts treat ISPs analogously to other telecommunications carriers. In this respect, almost any facilitation is sufficient for disclosure. Only a handful of cases have considered this issue. In *Coca-Cola Company v British Telecommunications plc*,[132] Neuberger J ordered the respondent telephone company to disclose the name and address of an accountholder who used his mobile telephone to coordinate the sale of infringing soft drink syrups to hoteliers. Facilitation was established because these telephone services were probably 'of central significance' to the delivery of infringing goods.[133] In this respect, BT's 'degree of mixing up' in primary wrongdoing was slight: it never took possession of infringing goods, and the phone was used predominantly for non-infringing activities; it merely supplied lawful services which were used to effect the subscriber's scheme. Neuberger J accepted that this was 'a less strict view' of the traditional facilitation requirement. By analogy, it appears that where an ISP's services are a 'central' or 'essential' element in the commission of a tort, it will be taken to have facilitated the tort in a manner sufficient for *Norwich Pharmacal* disclosure.

(b) *Evidence of wrongdoing*

Most applications for disclosure rely upon IP addresses collected by rights-monitoring companies using automated technical processes. Courts tend to accept this evidence at face value.[134] *DigiProtect Gesellschaft Zum Schutze Digitale Medien GmbH v BE UN Ltd*[135] is a typical case. There

---

[132] [1999] FSR 518 ('*Coca-Cola*').

[133] Ibid 524 (Neuberger J).

[134] See, eg, *EMI v Eircom Ltd* [2005] 4 IR 148, [6] (Kelly J) (*prima facie* evidence of infringement); *BMG Canada*, [35] (Sexton JA) (genuine claim of primary wrongdoing).

[135] [2008] (Unreported, High Court of Justice, Chief Master Winegarten, 30 June 2008).

the claimant was a digital enforcement company which used BitTorrent monitoring software to compile a list of IP addresses from which copyright works had been uploaded, and sought disclosure of their identities from nine English ISPs. Disclosure was granted summarily, with all costs to be paid by the applicant.[136]

Media CAT Ltd v Adams illustrates the difficulties that can arise.[137] The applicants purported to be 'representatives' of various copyright owners from whom they licensed the right to enforce copyright against infringers in return for a share of damages recovered. Using proprietary technology, the applicants determined that some 30 000 IP addresses on the respondents' networks were sharing the licensed works using P2P file-sharing applications. The works were all pornographic in nature. In an unreported decision, Chief Master Winegarten ordered Plusnet plc to disclose the name and address of the subscriber to whom each IP address was assigned at the relevant time.[138] The applicants did not allege that the ISPs were liable, but it was not disputed that the ISPs facilitated subscribers' infringements and were therefore mixed up in wrongdoing. In another unopposed application, BT was ordered to disclose similar information.[139]

The ISPs gave disclosure. However, instead of bringing proceedings against the identified third parties, the applicants then commenced a letter-writing campaign of considerable magnitude. Their letters demanded a settlement fee — typically £495 or £800 — as 'compensation' for infringement and costs, in return for which the matter would be taken no further and their identities kept private. The applicants' solicitors, who were entitled to 65 per cent of recoveries, sent letters which materially misrepresented the applicants' case and did not sufficiently explain that no finding of actual infringement had been made. Unsurprisingly, many recipients paid up — though it is unclear just how many. Of those who did not, only 27 actions were commenced, and after failing to obtain *ex parte* judgment[140] the applicants sought discontinuance of the actions and took no further steps to advance them. The notices of

---

[136] See also *Topware Interactive Inc v Barwinska* [2008] PAT08023 (Unreported, Patents County Court, HHJ Fysh QC, 22 July 2008).

[137] [2011] FSR 28 ('*Media CAT*').

[138] *Media CAT Ltd (Phase 2) v Plusnet plc* (Unreported, High Court of Justice, Chief Master Winegarten, 19 November 2009). (Plusnet allocates IP addresses dynamically, and must cross-check data against its historical records.)

[139] *Media & More GmbH & Co KG v British Telecommunications plc* (Unreported, High Court of Justice, Warren J, 27 January 2010).

[140] *Media CAT Ltd v A* [2010] EWPCC 017.

discontinuance were later struck out as an abuse of process, since the applicants lacked standing and their collateral purpose was to prevent the claims from ever being tested in court.[141]

Media CAT is an unfortunate example of how seemingly uncontroversial disclosure orders can be misused on a vast scale. The remedy of disclosure was used to perpetrate a scheme in which parties were given no realistic prospect but to submit to a demand of payment for a wrong for which they may or may not have been responsible, where liability was never determined by a court.[142] This is all the more concerning because the claims raised novel questions of law and relied upon untested evidence.[143] The entity issuing the demand lacked title to sue, was unconnected with the proper claimant and removed from the incentive structure contemplated by copyright law. As can be seen from the enormous quantity of critical discussion online,[144] the use of disclosure for this purpose is liable to undermine public confidence in the administration of justice and to bring the legal profession into disrepute.[145] The fact that serious injustice can be caused by improper use of identity information underscores the importance of placing appropriate limitations upon disclosure.[146] Although there are good reasons to encourage *bona fide* attempts at settlement, demanding sums far in excess of the applicants' likely losses under threat of public humiliation is arguably not a legitimate purpose for disclosure.

Media CAT is far from the only example of 'speculative invoicing'.[147] However, courts are scrutinising the use of *Norwich Pharmacal* orders more closely. In *Golden Eye (International) Ltd v Telefónica UK Ltd*,[148] the first claimant sought disclosure of the identities associated with 9124 IP addresses, from which it alleged that the subscribers had infringed its copyright by uploading or downloading the claimants' pornographic films using BitTorrent. The first and second claimants owned some copyrights in their own right; the remainder had been licensed under an arrangement with the other 12 claimants whereby the first claimant would receive up to 75 per cent of damages recovered from internet infringers. It proposed to send letters to each subscriber offering to settle

---

[141] *Media CAT Ltd v Adams [No 2]* [2011] FSR 29, 724–5 (HHJ Birss QC) ('*Media CAT [No 2]*'); *Media CAT*, 707–9, 711 (HHJ Birss QC) (failure to join copyright owner and assign rights).

[142] Cf *Intercen*, where liability was ruled upon following disclosure.

[143] *Media CAT*, 691–2 (HHJ Birss QC).

[144] See, eg, 'Hickster', 'Received a Letter from ACS Law?' (2009) <http://acsbore.wordpress.com/>; 'Penumbra', 'DL/ACS:Law — I've Received a Letter, What Should I Do?' (21 November 2008) <http://www.slyck.com/forums/viewtopic.php?p=494241>; Anonymous, 'Being Threatened?' (2011) <http://beingthreatened.com/>.

[145] See *Media CAT [No 2]*, 735–6, 740–1 (Birss J) (making wasted costs orders).

[146] Cf *Topware Interactive Inc v Barwinska* [2007] (Unreported, High Court of Justice, Master Behrens, 1 February 2007) [2] (purpose of disclosure unrestricted).

[147] See, eg, BBC, 'Game Sharers Face Legal Crackdown' (19 August 2008) <http://news.bbc.co.uk/1/hi/technology/7568642.stm>.

[148] [2012] EWHC 723 (Ch) ('*Golden Eye*').

claims for £700. The defendant ISP did not oppose the order or make submissions. However, Consumer Focus, a consumer watchdog, intervened on behalf of the affected subscribers.

Arnold J granted disclosure to the first and second claimants, but refused relief to the remaining 12 claimants. The traditional *Norwich Pharmacal* requirements were clearly established, there being a good arguable that 'many, but not all' of the subscribers had committed copyright infringement at the identified IP addresses, which the ISP had facilitated.[149] Disclosure was 'plainly necessary' to enforce the claimants' copyrights,[150] though there would inevitably be some percentage of identified subscribers who were not infringers (for example, due to errors in the ISP's records or because someone else was using the relevant connection). In light of the large number of potential defendants and the low value of each claim, it was unnecessary for the claimant to intend to pursue every infringer: merely sending pre-action letters was a legitimate purpose since motivated by a 'genuine commercial desire … to obtain compensation'.[151] In these circumstances, the claimants were *prima facie* entitled to disclosure, subject to an analysis of proportionality. This issue will be considered below.

(c) *Privacy interests of subscribers*

In *Golden Eye*, privacy was treated as a question of balancing the competing rights of copyright owners and users. Arnold J adapted the traditional approach, placing 'an intense focus' on the relative importance of each party's right and the justifications for interference, before applying the 'ultimate balancing test' of proportionality.[152] Relevant here was the fact that most subscribers were retail consumers who may be innocent of any wrongdoing. Further, the pornographic nature of the subject matter at issue may cause embarrassment or distress, and lead recipients to settle unmeritorious claims. Notwithstanding these factors, the claimants' legitimate need to enforce their property rights — whose infringement was widespread — still outweighed the subscribers' privacy rights. Disclosure was accordingly proportionate if appropriate safeguards were adopted to protect subscribers' rights and, in particular, those who were innocent of wrongdoing.[153]

The most important safeguard was the Court's supervision of pre-action correspondence to ensure that it is not misleading or otherwise objectionable. Arnold J excised several passages from

---

[149] Ibid [103]–[105] (Arnold J).

[150] Ibid [115] (Arnold J).

[151] Ibid [109] (Arnold J).

[152] Ibid [116]–[117]. See also *In re S (a child)* [2005] 1 AC 593, 603 (Lord Steyn).

[153] *Golden Eye*, [145].

the proposed letters of demand, including the specific sum of money claimed in settlement (since the precise loss claimable from each recipient would vary, and might in some cases be zero), and required other passages to be written in more restrained language.[154] This supervisory role is clearly important if abuse is to be prevented. Additionally, Arnold J recommended the selection of 'suitable test cases' by the claimants so that common issues could be determined at an early stage before an appropriate tribunal.[155] Finally, Arnold J refused to order disclosure for copyrights licensed to the first claimant, since to permit aggregation of disclosure rights in return for a share in recoveries 'would be tantamount to the court sanctioning the sale of the [subscribers'] privacy and data protection rights to the highest bidder'.[156] The Court of Appeal overturned this restriction, since the licence agreements were not champertous and there was, strictly speaking, no 'sale' of privacy rights. Arnold J's restriction would have placed clear limits on the ability for copyright owners to enter into business arrangements with third parties to litigate on their behalf. While it would not prevent those parties from seeking disclosure directly, it would effectively reduce the potential for large-scale disclosure applications.[157] It is regrettable that the Court of Appeal has removed the only effective limitation on large-scale commercial disclosure.

3.4 Search engines

Only one case has considered the duty of search engines to disclose information about tortious activity.[158] In *Grant v Google UK Ltd*,[159] Rimer J ordered Google to disclose information identifying a keyword advertiser who had placed AdWords listings on Google's search engine. The advertisements directed users to a website containing infringing material, which used a domain name cloaking service to shield the registrant's identity.[160] Google did not oppose disclosure but refused to do so voluntarily, citing its privacy policy.[161] *Grant* is therefore a good example of how *Norwich Pharmacal* orders can facilitate meaningful relief. The infringing website had already been suspended after complaints were made to its host, but the claimant also sought

---

154 Ibid [123]–[138].

155 Ibid [143]–[144] (Arnold J).

156 Ibid [146] (Arnold J).

157 Cf *BMG Canada*, [41] (Sexton JA) (Richard CJ and Noël JA agreeing) ('privacy concerns … must yield to public concerns for the protection of intellectual property rights').

158 Although a second reported decision exists involving Google Inc as a respondent, that case involved the company in its capacity as a host of emails: see above § 3.2.

159 *Grant v Google UK Ltd* [2005] EWHC 3444 (Ch).

160 Ibid [6]. Costs of disclosure were borne by the claimant.

161 See Google Inc, 'Privacy Policy' (20 October 2011) *Google Privacy Center* <http://www.google.com/intl/en/privacy/privacy-policy.html>.

monetary relief for losses caused by the infringements. In this way, disclosure supported her primary remedy even after the tortious content had been removed.

A more pressing but hitherto unexamined issue is whether *Norwich Pharmacal* orders can be used to obtain details of an individual's search history. Such data are commonly stored for the purposes of algorithm improvement, behavioural advertising, personalised results and law enforcement. Its usefulness to claimants is obvious: it might show a browsing trail leading to infringing content, disclose upload or publication activity or simply reveal a party's state of mind at a particular time. Because people tend to use search engines as a research tool of first resort, this information is becoming increasingly sensitive. Even when data are retained in an anonymised format, identification is possible by aggregating fragments about an individual's location, workplace, and demographics.[162]

Although the matter has not yet arisen for decision, it is suggested that courts should be slow to acquiesce to such requests. First, search data invite fishing expeditions and necessarily involve disclosing data beyond the identity of the tortfeasor — something the *Norwich Pharmacal* procedure was never designed to accomplish.[163] It would be difficult to limit the scope of disclosure to tortious activity, since search histories — even within a given date range and keyword set — may include many unrelated activities. Second, users can demonstrate strong expectations of privacy in respect of their search queries.[164] The privacy policies of Google and other search engines reinforce this belief in the sanctity of search data. Users' query behaviour suggests that they regard their search queries as visible by them alone (a conclusion suggested by the relatively high volume of queries for adult material compared to the prominence of public requests for such material). Unlike commenters on public bulletin boards, search engines are not public fora, so the rationale offered in *Totalise* does not apply.

Third, to disclose private browsing histories is disproportionate when the browsing history rarely if ever itself constitutes a tort. Querying a search engine is a mere preparation for tortious activity; it may trigger the display of tortious material or references to it, but will not of itself

---

[162] See, eg, Kelly Martin, 'AOL Search Data Identified Individuals' (8 September 2006) *Security Focus* <http://www.securityfocus.com/brief/277>.

[163] The framework of third party disclosure under pt 31 of the *Civil Procedure Rules* is better equipped to place appropriate limitations on the scope and format of such an exercise.

[164] See Aleksandra Korolova et al, 'Releasing Search Queries and Clicks Privately' (Paper presented at International World Wide Web Conference, Madrid, 20–24 April 2009) <http://www2009.eprints.org/18/1/p171.pdf>; Christopher Soghoian, 'My FTC Complaint about Google's Private Search Query Leakage' (7 October 2010) *Slight Paranoia* <http://paranoia.dubfire.net/2010/10/my-ftc-complaint-about-googles-private.html>. Cf Evelyn Kao, 'Making Search More Secure' (18 October 2011) *The Official Google Blog* <http://googleblog.blogspot.com/2011/10/making-search-more-secure.html>.

constitute any known tort which the search engine facilitates.[165] Finally, there is a real argument that disclosure would inhibit candour between users and their search engines, which would correspondingly diminish their ability to access information freely — a recognised component of the right to freedom of expression. Such a result would be concerning because, in an age where a search engine is an extension of the inquiring mind, it leads to the undesirable result that users self-censor their thoughts or go without access to information they may have a legitimate interest in receiving.

3.5 Social networks

Applications for disclosure against social networks fall to be determined according to conventional principles. In *Applause Store*, the Court ordered disclosure of information relating to defamatory postings on Facebook. These activity logs included various time-stamped events such as when the defendant logged in and out from an account and posted content, which were instrumental in the Court's conclusion that he was responsible for the postings.[166] While *Applause Store* illustrates the forensic utility of disclosure from social networks, it also highlights the creeping scope of identity information. Identity in the narrow sense involves names and contact details; in the broad sense used in *Applause Store*, it implicates a growing sphere of circumstantial data which are sufficient to pinpoint one person as the author of the tortious material and reconstruct a version of events which supports the claimant's case. In one sense, this is a logical progression: *Norwich Pharmacal* relief is designed to be pragmatic, and should include all information 'necessary' to pursue the tortfeasor; however, it also raises concerns about the proper scope of social identity data, much of which will be irrelevant to the tort. Disclosure against social networks has also been used to unmask the perpetrators of campaigns of social harassment[167] and threatening emails sent to Members of Parliament.[168]

3.6 Data retention duties

Disclosure is only a useful remedy if the defendant possesses relevant information. Due to the volume of data processed by internet intermediaries, it is rare for all records to be retained.

---

[165] Cf *Coca-Cola*, 524 (Neuberger J).

[166] *Applause Store*, [65]–[68] (HHJ Parkes QC).

[167] See also BBC, 'Facebook to Release ID of Users Who Abused Woman Online' (7 June 2012) <http://bbc.co.uk/news/uk-england-sussex-18351855>.

[168] Steven Morris, 'Louise Mensch "Troll" Sentenced over Threatening Email' (*The Guardian* 11 June 2012) <http://guardian.co.uk/uk/2012/jun/11/louise-mensch-troll-sentenced-email>.

Instead, access logs and other data tend to be cycled and automatically erased at regular intervals. This means that a potential claimant may have a limited window within which to seek disclosure and thereby be in a position to commence proceedings; it is a *de facto* limitation period that can be extremely oppressive to claimants who do not discover the tortious material until long after its publication. Nevertheless, intermediaries will often store data over longer periods for commercial or technical reasons, or because obligated by law.

Data retention is a statutory duty imposed upon notified 'public communications providers'[169] — ISPs, hosts and other network layer intermediaries — to retain traffic, location and related data necessary to identify each user.[170] These duties do not arise to correct wrongdoing by an intermediary but rather to facilitate the investigation of serious crime.[171] Unlike disclosure, retention is indiscriminate but of limited duration. A full examination of the attendant proportionality and privacy issues is beyond the scope of this chapter,[172] but two aspects are relevant to intermediaries' duties of disclosure.

(a) *Scope of retainable data*

First, the effect of the Data Retention Directive and its transposing legislation is to ensure that intermediaries hold a full complement of data which might be made the subject of a timely application for disclosure. For example, the *Regulation of Investigatory Powers Act 2000* (UK) imposes obligations on telecommunications service providers to store 'traffic data', which includes subscriber information, electronic routing information and the source and destination of internet communications traffic. Although only metadata need be retained (and not the communications themselves), retention is extensive:[173] it includes the source and destination of all emails, web browsing history and IP addresses. However useful this information may be to law enforcement authorities, it represents a treasure trove to private litigants.

---

[169] *Data Retention (EC Directive) Regulations 2009* (UK) reg 10(1) ('*Data Retention Regulations*').

[170] *Data Retention Regulations* regs 2(b), 4(1); Data Retention Directive arts 3(1), 5(1).

[171] European Commission, *Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)* (2011) 1, 3.2.

[172] See further Ian Brown, 'Communications Data Retention in an Evolving Internet' (2011) 19 *International Journal of Law and Information Technology* 95.

[173] See *Home Office Voluntary Code*, appendix A; *Anti-terrorism, Crime and Security Act 2001* (UK) s 102.

(b) *Use of retained data for private purposes*

Second, although the use of intercepted data is restricted in various ways,[174] little regard has been paid to disclosure of retained data for private purposes in civil proceedings. In general, retained data may not be disclosed to any person except in specific cases and where 'permitted or required by law'.[175] Most authorised disclosures are to specified public authorities for narrow public purposes, such as national security, preventing or detecting crime,[176] enforcing trade practices legislation,[177] or 'in pursuance of an EU obligation'.[178] The focus on the public purposes for which data may be disclosed has obscured the inevitability that such data are made available to private litigants in *Norwich Pharmacal* proceedings. Courts do not appear to inquire as to the reason why the information was retained or whether disclosure is permitted under any enactment.[179] Indeed, the contrary assumption is reflected in paragraph 28 of the *Voluntary Code*, which states that access requests 'can also be received' from civil litigants and data subjects.[180]

Although this information leakage represents a substantial increase in the scope of retention, it appears to be lawful. The CJEU recently validated the practice in *Bonnier Audio AB v Perfect Communication Sweden AB*,[181] where it concluded that national laws permitting disclosure of retained communications data were compatible with the Data Retention Directive provided that they enabled a 'fair balance' to be struck between the competing fundamental rights. This would be so where a national court could weigh the 'conflicting interests' and consider the costs and benefits of disclosure in a given case.[182] Judicial assessments of proportionality in *Norwich Pharmacal* proceedings arguably satisfy this requirement.

---

[174] See *Telecommunications (Data Protection and Privacy) Regulations 1999* (UK); *Official Secrets Act 1989* (UK) s 4(3)(a) (prohibiting disclosure of retained or intercepted information).

[175] *Data Retention Regulations* reg 7. See, eg, *Regulation of Investigatory Powers Act 2000* (UK) s 22(2).

[176] See, eg, *Anti-terrorism, Crime and Security Act 2001* (UK) s 17(2), sch 4.

[177] *Telecommunications Act 1984* (UK) ss 45, 101(2)(d), 101(3).

[178] *Telecommunications Act 1984* (UK) s 101(2)(e).

[179] One possibility is that disclosure is required in intellectual property cases 'in pursuance of an EU obligation' under the Enforcement Directive: see below §4.1.

[180] *Home Office Voluntary Code*, [28].

[181] Case C-461/10 [2012] 2 CMLR 42.

[182] Ibid [58]–[59].

4 Disclosure as a complementary remedy

So far this chapter has considered the scope of disclosure which internet intermediaries must give to claimants. This section argues that the equitable duty is justified as the logical corollary of excluding intermediaries' monetary liability for mere facilitation. An obligation to give disclosure is the price which must be paid for that immunity. However, there are good reasons for disclosure not to be an overriding duty. The existing framework offers limited protection to the rights of internet users and intermediaries. Several procedural reforms are suggested which better safeguard those interests, while retaining the remedy's important function of preserving access to justice. For clarity, it is not suggested that existing equitable principles should be abandoned; nor should any different principles apply in cases involving internet wrongdoing. Instead, these reforms are intended as subtle but important tweaks to the manner in which courts conduct their proportionality assessment to preserve some forms of anonymous speech.

4.1 Compatibility with European law

At least in the context of intellectual property, an effective disclosure remedy is essential to comply with European law. These obligations affect *Norwich Pharmacal* applications in two ways. First, they place lower limits on relief by requiring that the procedure be available, effective and part of a system of remedies to prevent certain torts from continuing. Second, they place upper limits on relief by requiring that disclosure be proportionate, necessary and compatible with fundamental rights. These maximum standards are especially important online because of the potential for excessive disclosure to chill speech and intrude upon the right to private life. They indicate that the public policy of access to justice is not absolute, and must occasionally yield to other interests — even at the expense of claimants' rights.

(a) *Minimum standards*

The importance of *Norwich Pharmacal* relief arises partly because, as a form of injunction, it is exempted from the safe harbour regime. Recital (45) of the E-Commerce Directive recognises that intermediaries are not relieved of their obligations to comply with 'injunctions of different kinds'. To the contrary, article 18 requires member states to make interim measures available to 'terminate any alleged infringement' and prevent 'any further impairment of the interests

involved.' Disclosure is therefore arguably necessary to give effect to article 18,[183] since without access to the defendant's identity those measures may be ineffective. In copyright cases, article 8(1)(c) of the Enforcement Directive requires disclosure to be available against a party who supplies 'services' used in infringing activities on a commercial scale. As articles 9(1)(a) and 11 also make clear, claimants must also be able to obtain injunctions against intermediaries whose services are used to infringe.[184] In *eBay*, Arnold J considered that article 11 required the protective jurisdiction to be extended to a marketplace intermediary which facilitated trade mark infringements.[185] In this way, European law provides an expansionist influence upon the Court's jurisdiction to order disclosure.

(b) *Maximum standards*

As discussed in chapter 3, injunctions against intermediaries are subject to limits. A disclosure order could be incompatible with European law if failed to respect those limits — for example, by not striking a fair balance between the parties' fundamental rights, or by being disproportionate or excessively costly. In *Scarlet*, the Court rejected the national injunction because it required 'systematic analysis' of users' IP addresses, which are personal data that uniquely identify individuals.[186] Although that analysis was limited to arguable tortfeasors (alleged uploaders of infringing material) it was still disproportionate. It remains unclear to what extent *Norwich Pharmacal* orders are subject to the same restrictions outside intellectual property cases,[187] but they are likely to be compatible with European law on any view. First, disclosure is much more limited in scope and duration than rolling monitoring, since it concerns specific users and records held at a particular point in time. Even disclosure of the scale seen in *Media CAT* and *Golden Eye* is orders of magnitude less than the data analysis required by *Scarlet*.

Second, although disclosure interferes with the right to privacy by identifying individuals, it is necessary and proportionate to a legitimate aim; namely, preserving the right to a fair trial.[188] Judicial scrutiny ensures that disclosure procedures contain 'adequate and effective safeguards

---

[183] See also *Anti-Counterfeiting Trade Agreement*, opened for signature 1 May 2011 (not entered into force), arts 2.18(4) (disclosure against internet intermediaries), 27.4 (disclosure of ISPs' subscriber information).

[184] Enforcement Directive arts 9(1)(a), 11. See also Information Society Directive article 8(3).

[185] *eBay*, 785 (Arnold J).

[186] *Scarlet* [41].

[187] See *Newzbin2*, [27]–[30], where Arnold J appeared to distinguish the *Norwich Pharmacal* jurisdiction from injunctions under article 8(3) because only the latter confers 'a legal right to the substantive remedy of a final injunction'. Such a distinction is inconsistent with the traditional treatment of disclosure as a final remedy.

[188] See, eg, *McMichael v United Kingdom* (1995) 20 EHRR 205, [87]. Upholding the right to property was accepted in *Scarlet* as a legitimate aim, though not an inviolable one: *Scarlet*, [42]–[44].

against abuse'.[189] As the CJEU held in *Bonnier*, any disclosure procedure which accommodates a discretionary assessment of proportionality and 'weigh[s] the conflicting interests' is likely to strike a fair balance.[190] Third, disclosure is normally a minor expense for intermediaries compared to the filtering obligations imposed by the national court in *Scarlet*. Fourth, unlike the DPI system in *Scarlet*, properly delimited disclosure orders do not involve scrutiny of the contents of electronic communications — only the use of identity metadata (typically IP addresses and contact information). Finally, unlike blanket monitoring, disclosure orders distinguish between lawful and unlawful content by first requiring proof of a reasonable allegation of wrongdoing. It therefore seems likely that *Norwich Pharmacal* disclosure can reflect a 'fair balance' of rights that is compatible with European law, though ultimately this assessment depends on the scale, purpose and subject matter of disclosure that is sought in a particular case.

4.2 Effectiveness

To say that disclosure complements or reflects the limits of monetary liability means that it can be thought of as the price which must be paid in return for immunity under safe harbours, defences and other doctrines limiting secondary liability. If a facilitator of wrongdoing is not liable to pay compensation, then it follows that he should point the victim in the direction of someone who is. Duties of disclosure ensure that the party left holding the key to the claimant's remedy must act in a way which promotes, rather than negates, the claimant's substitutive rights. They reflect a policy compromise between absolute immunity for conduits, which would harm claimants, and broader rules of secondary liability, which would harm conduits. This middle ground recognises that intermediaries can be part of a loss-shifting mechanism without recourse to liability rules which offer the binary choice between 'liability' and 'no liability'. Instead, the equitable jurisdiction functions as a flexible lever which allows courts to apportion costs and regulate users' anonymity in individual cases. This approach has numerous benefits.

(a) *Pursuing internet wrongdoers*

Disclosure is a powerful tool for claimants in cases involving internet intermediaries. Because of the ease with which internet torts can be committed anonymously, disclosure is often essential for claimants to identify a suitable defendant and obtain redress. It is no coincidence that the

---

[189] *Funke v France* (1993) 16 EHRR 297, [56].

[190] *Bonnier*, [60]; approved in *Viagogo (SC)*, [40]..

defamatory comments in *Tamiz*, *Godfrey* and *Totalise* were made anonymously;[191] and that the file-sharers and tracker operators in *iiNet*, *Newzbin* and *Dramatico* were anonymous. In *Viagogo*, the Supreme Court emphasised that the marketplace allowed people 'anonymously to sell event tickets',[192] much as *eBay* affords partial anonymity during registration.[193] Self-evidently, primary wrongdoers do not willingly advertise their identities. To the contrary, they take active steps to conceal them. Frequently, it is only possible to unmask such a person by assembling myriad data held about them by their ISPs and other intermediaries. Not without justification, most data controllers refuse to reveal their customers' identities without a valid court order. It is clear that a robust and efficient disclosure procedure is necessary to assist claimants in unravelling the tangled web of identity information contained in IP addresses, usernames and pseudonymous email accounts scattered among multiple intermediaries, each of whom possesses one necessary but insufficient piece of the puzzle.[194] Equally, because *Norwich Pharmacal* orders make it possible to triangulate internet users in precisely this way, care is required to ensure that such an invasive remedy is not misused.

The availability of disclosure indirectly reduces pressure on intermediaries to provide a substantive remedy by offering up a party who is more closely connected with harm. Without disclosure, relief against the primary tortfeasor would be impossible or impracticable and the intermediary may be named in their place.[195] In this way, disclosure complements safe harbours and reinforces the limits of secondary liability by improving the likelihood that the primary wrongdoer can be pursued. Disclosure thus preserves the status of intermediaries as innocent facilitators who are 'mixed up in wrongdoing' rather than obligated to police or compensate it.

(b) *Regulating anonymity*

An injunctive remedy is vitally important because intermediaries may otherwise be bound by obligations of confidence which prevent them from disclosing users' identities. While terms of service can be used to limit or exclude confidentiality, intermediaries have little incentive to widen their enforcement obligations and may face criminal liability if they voluntarily disclose

---

191 *Tamiz (CA)*, [7] (Richards LJ); *Godfrey*, 205 (Morland J); *Totalise*, 1235 (Aldous LJ).

192 *Viagogo (SC)*, 3336 (Lord Kerr JSC).

193 *eBay*, 715 (Arnold J) (noting that users could supply an anonymous email address, subject to payment verification).

194 This reflects the decentralised design of the Internet: see above chapter 2, § 3.2.

195 One can easily imagine such an approach being taken in *Viagogo*; cf *eBay*, above chapter 3, § 1.3(b)(v).

telecommunications data.[196] The availability of compulsory disclosure is therefore a necessary antidote to the secrecy of communications which intermediaries are increasingly required to protect. For similar reasons, potential claimants are unable to use self-help mechanisms to locate the defendant because of the risk of criminal liability for intercepting and disclosing transmitted telecommunications data.[197] In this way, the *Norwich Pharmacal* jurisdiction regulates anonymity by appointing courts to supervise intermediaries in their roles as proxy gatekeepers of internet users' identities.

Set against these benefits, the development of new encryption and IP obfuscation technologies will eventually reduce the amount of useful identity data retained by intermediaries. The data retention and disclosure framework currently fails to make provision for encrypted communications, whose security continues to increase relative to the available counter-measures. However, the fact that disclosure cannot offer a complete solution to wrongdoing on the internet does not discount it as a valuable tool for pursuing tortfeasors in appropriate cases. As discussed in chapter 7, disclosure forms just one of a number of mechanisms which protect rights online.

(c) *Flexibility and transparency*

Disclosure involves a public compromise between discretion and supervision. The remedy's 'open and flexible nature'[198] focuses attention on the complex factoring of interests implicated in wrongs carried out using new technologies. This discretion is desirable in an environment in which the types and method of wrongdoing are constantly evolving. Conversely, judicial supervision compensates for the fact that intermediaries have no direct interest in protecting their customers' rights, least of all those accused of wrongdoing. Unless the intermediary is unusually dedicated in its assessment of the allegations,[199] a professional tribunal is likely to make more reliable decisions and better accommodate the rights of third parties than one motivated only by expedience and self-interest. A judicial procedure upholds the rule of law by ensuring that even a preliminary determination of the claim is conducted in accordance with law by a competent tribunal. This legitimates what might otherwise be a misuse of private information. Consistent

---

[196] See *Privacy and Electronic Communications (EC Directive) Regulations 2003* (UK) reg 6; *Telecommunications (Data Protection and Privacy) Regulations 1999* (UK) regs 6, 33. But note that disclosure is possible where necessary for 'exercising or defending legal rights', even if proceedings have not been commenced: reg 33(b)(iii).

[197] See *Regulation of Investigatory Powers Act 2000* (UK) s 1.

[198] Stuart Paterson and Anna Fitzherbert, 'From Guantanamo Bay to Outer Space: Developments in *Norwich Pharmacal* Relief' (2010) 29 *Civil Justice Quarterly* 38, 47.

[199] Eg, Google has stated that it will not disclose information unless it has concluded a process of internal review to determine that disclosure would not contravene its privacy policy: Interview, Jenni Aldrich, Regional Legal Director, Google Australia Pty Ltd (19 December 2011, Sydney).

with the principle of open justice, *Norwich Pharmacal* hearings are listed and, in all but the most exceptional cases, open to the public. The resulting attention[200] holds claimants accountable; for example, one popular music publisher withdrew its application after widespread criticism from customers.[201]

The downside of requiring a formal application is that it entails higher costs for claimants. To encourage voluntary disclosure, it is said, would be more consistent with the policy that parties be encouraged to settle their differences outside court. The problem with this argument is that it has in mind consensus being reached between two litigants who have roughly equal stakes in a dispute; this is not true of claims where the intermediary has no direct interest in the information being disclosed. An intermediary that capitulates to a private demand for disclosure does not settle the primary dispute — indeed, it catalyses further litigation — and acts without the procedural and evidentiary legitimacy of a court. In any case, the Court's intervention may actually reduce cost by consolidating parallel disclosure applications and determining contested issues at an early stage. Where thousands of users are involved, active case management is desirable to prevent disclosure from becoming unmanageable.[202]

(d) *Enforcement costs*

Despite its strengths, it is clear that disclosure cannot solve the problems of widespread internet wrongdoing on its own. It can be expensive to obtain, as Charleton J observed in *Eircom*:

> this process is burdensome and, ultimately, futile as a potential solution to the problem of internet piracy. [One witness] has given evidence of the time, trouble and expense involved in the pursuit of this remedy. … To identify 17, 49 and 23 names, through the three cases seeking *Norwich Pharmacal* orders, cost €680,000 to pay solicitors and barristers on all sides. Some settlements were effected, returning €80,000.[203]

Existing disclosure procedures 'are indiscriminate, costly and inefficient', and take no account of the degree of care exercised by an intermediary for the purpose of determining costs.[204] One partial solution, discussed in chapter 5, is to disclose anonymised data about infringers to inform a determination of which are worth pursuing. Another solution, proposed in chapter 8, is to establish specialised tribunals for targeted, cost-effective disclosure under a standardised process.

---

[200] See, eg, Various contributors, 'Plusnet will give your personal details to ACS Law …' (7 May 2010) *Plusnet Forum* <http://community.plus.net/forum/index.php/topic,85908.0.html> (over 2000 messages from retail consumers concerned about identity disclosure).

[201] See, eg, Josh Halliday, 'Ministry of Sound Suspends Filesharing Action' (*The Guardian*, 3 November 2010) <http://guardian.co.uk/technology/2010/nov/03/ministry-of-sound-filesharing-bt>.

[202] See, eg, *Smith v ADVFN plc* [2008] EWCA Civ 518, [14] (May LJ) (Moore-Bick LJ agreeing).

[203] *Eircom*, [62] (Kelly J).

[204] *BT*, [238] (Parker J).

However, even where granted it will rarely be feasible or palatable for a claimant to take action against every suspected wrongdoer. The costs of pleading and proving each tort would quickly prove crippling to all but the most well-resourced of claimants, and there are obvious reputational costs in having to bring proceedings against customers, often in reliance upon unreliable identity evidence. The damages recoverable will rarely outweigh these costs, particularly where the scale of wrongdoing is small.

4.3 Proportionality

Cases such as *Media CAT* and *Golden Eye* demonstrate that the concept of proportionality can set meaningful limits on disclosure by requiring courts to assess the relative impact of disclosure upon internet users, claimants and intermediaries. Proportionality offers a flexible tool for balancing these parties' rights. At its simplest, it confirms the intuition that if the wrong is serious and the risk of misidentification low, disclosure is justified. If, however, the wrong is minor and the third parties are only speculative tortfeasors or may suffer serious irreparable harm from being identified, disclosure may be illegitimate. This calculus is an essential part of the exercise of the Court's discretion because it provides an opportunity to protect and encourage socially beneficial exchanges (and discourage undesirable ones) by ensuring that the uploaders of valuable material are less likely to be unmasked without good reason. Properly applied, proportionality ensures that the privacy of innocent parties is not unnecessarily invaded, and that probable wrongdoers are not intruded upon more than required.

However, courts must also be aware of the concept's limits. Proportionality fails to offer any universal criteria for balancing incommensurable interests. Weighing the relative impact of disclosure on privacy and freedom of expression against the need for a claimant to have access to justice cannot be done sensibly unless those two imperatives share a common unit of measurement.[205] The impact which disclosure has on an individual's right to private life cannot easily be measured — especially if their identity is unknown, since the precise degree of intrusion will depend on both their circumstances and the nature of the activity which the claimant seeks to attribute to them. Doubtless, in some cases there will be a common unit, as where the applicant suffers reputational or economic harm and disclosure would cause the same type of harm to the anonymous party. In many other cases, proportionality will offer an incomplete framework for

[205] See Timothy Endicott, 'Proportionality and Incommensurability' (Unpublished draft) (2012) 6.

assessing whether one outcome is preferable to another, which will require courts to develop additional criteria for weighing disclosure against privacy.

English courts have only partly embraced proportionality as a limitation on disclosure. As seen in *Viagogo*, proportionality often folds into an assessment of necessity, in that if disclosure is the only way a claimant can proceed, it tends to be considered proportionate regardless of the other consequences. Because *Norwich Pharmacal* relief, by its nature, tends to be sought in circumstances where there is no other source of the information, necessity fails to supply an independent limiting criterion (indeed, it merely repeats one of the elements for relief) and is conceptually redundant. If it be objected that no limiting criterion is needed, one should recall the potential inconvenience to 'mere witnesses' which provided the impetus for limiting equitable disclosure throughout its history. There is no reason to assume that those risks have entirely abated. Besides *Golden Eye*, very few courts have directly considered the impact of disclosure upon freedom of expression or made more than superficial efforts to balance the parties' rights. In many cases, courts disregard the rights of internet users entirely. Some possible solutions to these shortcomings are offered below.

(a) *Threshold for disclosure*

The standard to which claimants must prove wrongdoing has been progressively diminished by cases such as *Mohamed* and *Arab Satellite*. While this has the advantages of speed and economy for claimants, it is an imperfect disclosure heuristic which reflects a trade-off in favour of claimants as against publishers of material. More should be done to restrict disclosure to 'those who can reasonably be assumed to be wrongdoers'.[206] This requires consideration of the claimant's likelihood of success at trial, the availability of defences and the substantiality of wrongdoing. A lower threshold would make disclosure a cheap, fast remedy for anyone who wished to silence a critical voice on the internet. If claimants could unmask publishers by making allegations that, while arguable, are unlikely to succeed at trial, the mere threat of identification may be sufficient to deter anonymous authorship in ways that deprive the public of access to a much wider class of socially valuable expressions.[207]

Where the existence of primary wrongdoing is in doubt, achieving justice for both claimants and innocent third parties requires the Court to consider the probability that disclosure will

---

[206] *Norwich Pharmacal*, 179 (Lord Reid).

[207] See, by analogy, *Mobilisa*, 719. See also Eirik Cheverud, '*Cohen v Google, Inc*' (2010) 55 *New York Law School Law Review* 333, 352.

eventuate to be unjustified. For example, given that a relatively small percentage of defamation claims succeed,[208] the threshold for disclosure should aim to avoid 'trivial defamation lawsuits primarily to harass or to unmask' an anonymous critic.[209] The same is true of copyright, which relies on balancing and impression rather than bright lines of legitimacy.[210] Failing to accord a margin of deference to anonymous communications means that claims which lie just beyond the margins of wrongdoing are presumptively validated in a way that compromises freedom of expression and risks turning disclosure into a vehicle for harassment.[211]

Although a *Norwich Pharmacal* hearing is not the place for a full trial of the merits, the intrusiveness and potential chilling effects of disclosure justify two further threshold requirements. First, the Court should be satisfied of the primary claim at least to the standard of surviving summary dismissal;[212] that is, it must have a 'real prospect of succeeding'.[213] A similar uniform standard has been adopted by some United States courts.[214] Second, consistently with s 12(4) of the *HRA*, the Court should have regard to the importance of freedom of expression when considering whether to grant relief. Although s 12(3) does not apply (since publication is not directly being restrained), it suggests that the claimant's likelihood of success is a highly relevant factor in making that determination. Raising the threshold for disclosure will not adversely affect claimants because they will not be required to prove anything they would not already be required to prove at trial.[215] It merely makes the claimant prove his case 'at an earlier stage in the proceedings'[216] — the mirror image of the mere witness rule. The claimant's case will necessarily be incomplete; for this reason, success should only be linked to issues not involving the intended defendant's identity or subjective mental state. A successful claimant has been placed in no worse position than before, since he remains able to recover his costs from the wrongdoer or settle the

---

[208] See, eg, *British Chiropractic Association v Singh* [2011] 1 WLR 133.

[209] *Doe v Cahill*, 884 A 2d 451, 459 (Del SC, 2005).

[210] See, eg, *Bauman v Fussell* [1978] RPC 485, 487 (Birkett LJ), 490–2 (Romer LJ); cf *Temple Island Collections Ltd v New English Teas Ltd* [2012] EWPCC 1, [63]–[64] (HHJ Birss QC).

[211] See Anthony Ciolli, 'Technology Policy, Internet Privacy, and the Federal Rules of Civil Procedure' (2009) 11 *Yale Journal of Law and Technology* 176, 188.

[212] *Civil Procedure Rules* r 24.2(a)(i). See also Nathaniel Gleicher, 'Note — John Doe Subpoenas: Toward a Consistent Legal Standard' (2008) 118 *Yale Law Journal* 320, 325, 352.

[213] One obvious difficulty is the absence of any submissions from the respondent. Such submissions could either be made under the notification procedure suggested in §4.4 below, or the Court could require the applicant to make full and frank disclosure of any facts against them.

[214] See above nn 207–209.

[215] Cf Elizabeth Malloy, 'Bloggership: How Blogs Are Transforming Legal Scholarship: Anonymous Bloggers and Defamation: Balancing Interests on the Internet' (2006) 84 *Washington University Law Review* 1187, 1190–2.

[216] Ciolli, above n 211, 187.

primary claim with the benefit of preliminary findings. For this reason, a higher threshold is unlikely to retard legitimate attempts to resolve disputes.

(b) *Accuracy of disclosure*

Even if evidence pointing towards an email or internet account is possessed, that does not guarantee identification of the tortfeasor. While some data uniquely identify a single device to which only one person has access, the vast majority do not. As courts have pointed out in *Golden Eye* and *iiNet*, a public IP address is 'not necessarily' a specific person or computer and, at most, identifies an accountholder.[217] Identity data may reveal the holder of a shared subscriber account, an anonymous email address, an IP address which can no longer be matched to a particular subscriber, a shared device in a library, hotel or workplace, or an unsecured network or public access point which has been used by unknown persons. In some cases, the data may even be deliberately forged.[218]

Disclosure remedies are accordingly vulnerable to the criticism that they accept the accuracy of IP address data and assume an identity between device and wrongdoer. There is a strong argument for calling expert witnesses to verify the methodology by which the relevant evidence was collected. Even if accurate, courts deciding the primary claim will be required to draw inferences about use of shared user accounts, as in *Applause Store*. Courts must be aware of these evidentiary limitations and re-evaluate uncertainty as the identity 'arms race' between claimants and anonymous defendants continues to be waged. Australian and Canadian courts have insisted upon detailed examination of the technical evidence and its limitations.[219] It is concerning that few English decisions have addressed these issues in any detail.

(c) *Scope of disclosure*

The scope of disclosure bears on proportionality in two ways. First, the information which intermediaries are liable to disclose should not go beyond what is necessary to establish the intended defendant's identity. For example, in *Norwich Pharmacal*, their Lordships were mindful of floodgates arguments and the risk of 'fishing' by optimistic claimants who wished to seek out

---

[217] *iiNet (HCA)*, [16]; *Golden Eye*, [103]–[105] (Arnold J).

[218] Michael Piatek, Tadayoshi Kohno and Arvind Krishnamurthy, *Challenges and Directions for Monitoring P2P File Sharing Networks: or — Why My Printer Received a DMCA Takedown Notice* (2008) <http://dmca.cs.washington.edu/dmca_hotsec08.pdf>. See also Smith, above n 4, 447.

[219] See, eg, *iiNet*, [105]–[125] (Cowdroy J); *BMG Canada*, [20] (von Finckenstein J) (commenting that disclosure would be irresponsible without evidence that the data reliably identified the third party).

evidence to support a potential claim. Lord Cross dismissed such concerns because disclosure is solely of *identity* information and not the collection of evidence at large, which it was rightly assumed would be more time-consuming.[220] However, as noted above, modern cases seem to extend disclosure beyond mere identity and into the realm of substantive discovery. This is improper. The equitable jurisdiction was never designed to substitute or augment existing procedures for obtaining preliminary or non-party disclosure, but rather as a means of identifying the wrongdoer in order to take further action against them. As Suzor has argued, '[i]nformation and identity discovery perform different roles, and should not be confused or granted simultaneously'.[221]

In short, the scope of disclosure should be limited to specific wrongs and should exclude irrelevant personal information. In particular, it should avoid including non-identity evidence which reveals unrelated characteristics of the intended defendant. There is an inherent tension between the effectiveness of equitable disclosure from the claimant's perspective and the need to protect third parties from disproportionate requests. Claimants rightly consider that they should be entitled to obtain all relevant information to support their claim against a wrongdoer. However, while the equitable jurisdiction is clearly flexible and powerful, it lacks an effective procedure by which suspected wrongdoers can object to excessive disclosure, and no party before the Court has adequate incentives to object to irrelevant or privileged material.[222] Other forms of disclosure incorporate stronger safeguards for the protection of third parties' interests.[223] Absent exceptional circumstances such as fraud or urgency, those procedures should accordingly be used to obtain non-identity information.

(d) *The value of anonymous speech*

Another largely unexplored factor is the extent to which a public interest exists in maintaining the freedom to express impugned material privately. It is true that much of the internet's most offensive and harmful 'noise' is published anonymously.[224] Some intermediaries traffic in

---

[220] *Norwich Pharmacal*, 199 (Lord Cross).

[221] Nic Suzor, 'Privacy v Intellectual Property Litigation: Preliminary Third Party Discovery on the Internet' (2004) 25 *Australian Bar Review* 227, 256.

[222] See, eg, *Sony Music Entertainment (Australia) Ltd v University of Tasmania* [2003] FCA 532 (disclosure of entire web server given following two allegations of infringement, to identify potential defendants to unrelated claims).

[223] See *Civil Procedure Rules* rr 31.16, 31.17.

[224] See Saul Levmore, 'The Internet's Anonymity Problem' in Levmore and Nussbaum, above n 85 (ch 1), 50, 58–9.

anonymous postings, many of them tortious;[225] others make attribution mandatory to increase the 'signal-to-noise' ratio of valuable content.[226] Many anonymous contributions are authored by minors.[227] Their social and literary value varies enormously, but it is safe to say that attribution is more common for high-quality speech. Doubtless, much of the content that is published anonymously online is close to valueless, but other material makes invaluable contributions to intellectual and social life in ways that attributed material may not dare: it exposes wrongdoing,[228] holds governments and public authorities to account,[229] entertains and informs.[230] This is not accidental:

> Authors of political and critical opinion choose anonymity for a reason: to protect themselves against threats of intimidation and retaliation by the powerful interests those opinions indict.[231]

Many examples can be cited of how anonymity protects speakers and promotes valuable social policies: (1) whistleblowing by employees or public officials; (2) commentary and satire by prominent members of the public; (3) political polls; (4) teacher evaluations, product and business reviews; (5) public postings by children or vulnerable parties; (6) authors whose safety could be jeopardised by identification; and (7) victims of crime or harassment. As Aldous LJ noted in *Totalise*, 'there are many situations in which … the protection of a person's identity from disclosure may be legitimate.'[232] Rights to freedom of expression encompass both the named and the anonymous.

Noticeably absent from *Norwich Pharmacal* jurisprudence is any consideration of the reasons why alleged tortfeasors might choose to conduct themselves privately. To assert, as Owen J did in *Totalise*, that when an author chooses to express himself anonymously on a public platform he

---

[225] See, eg, Christopher Poole, 'What is 4chan?' (2012) <http://4chan.org/>; Matt Ivester, 'A Juicy Shutdown' (4 February 2009) *Official JuicyCampus Blog* <http://juicycampus.blogspot.com/2009/02/juicy-shutdown.html>.

[226] See, eg, Google Inc, 'Google+ Page and Profile Names' (2012) *Google+ Help* <http://support.google.com/plus/bin/answer.py?hl=en&answer=1228271 >; Amazon Inc, 'Pen Names and Real Names' (2012) *Help* <http://amazon.com/gp/help/customer/display.html?nodeId=14279641>.

[227] Daniel Solove, 'A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere' (2006) 84 *Washington University Law Review* 1195, 1196–7.

[228] See, eg, Anonymous, 'Secret Injunction Gagging *The Guardian* on Trafigura' (14 October 2009) *WikiLeaks* <http://wlstorage.net/file/minton-injunction.pdf>; David Leigh, 'Revealed: Trafigura-Commissioned Report into Dumped Toxic Waste' (*The Guardian*, 17 October 2009) <http://guardian.co.uk/world/2009/oct/17/trafigura-minton-report-revealed>.

[229] See, eg, Ian Reeves, 'Night Jack: The End of the Anonymous Blogger?' (16 June 2009) *Centre for Journalism* <http://centreforjournalism.co.uk/blogs/night-jack-end-anonymous-blogger>; Michael Peel, 'Night Jack Blog Loses Fight for Anonymity' (*The Financial Times*, 16 June 2009). See also *The Author of a Blog v Times Newspapers Ltd* [2009] EWHC 1358.

[230] See, eg, Jeremy Blachman, 'Anonymous Lawyer' (5 November 2009) <http://anonymouslawyer.blogspot.com/>. Cf Glenn Greenwald, 'The Distorting Effect of Anonymity' (12 March 2009) *Salon* <http://www.salon.com/2009/03/12/anonymity_2/>.

[231] Cheverud, above n 207, 357.

[232] *Totalise*, 1240 (Aldous LJ).

runs the risk that his identity will be unmasked, ignores those reasons. This is not to say that anonymous speech is always, or even frequently valuable; on the contrary, the 'shield of anonymity'[233] will often assist tortious conduct while making little or no contribution to matters of public interest. However, the potential value of anonymity in a particular case is relevant to determining which set of interests should enjoy priority.

(e) *Arguable wrongdoing and privacy*

The decisions in *Viagogo* and *Golden Eye* assume that privacy rights are not engaged where data identify arguable wrongdoers. This approach suffers from the obvious circularity that data reveal arguable wrongdoing whenever wrongdoing is argued to have occurred, which is tantamount to saying that privacy interests can never trump an allegation of wrongdoing — however tenuous the claim or otherwise strong the expectation of privacy. It is, of course, reasonable to suggest that internet users should not be able to wear the mantle of privacy to conceal actual or suspected invasions of others' rights. However, even tortfeasors may be entitled to expect privacy in respect of their private information. First, they remain entitled to protection of data which concern unrelated non-tortious activities (such as details of private correspondence or internet activity). Second, even if they have no legitimate interest in obscuring their identities *as against a claimant* (or an intermediary), they might still expect privacy from third parties.

The Court's willingness to permit disclosure in *Viagogo* is better explained in two ways. First, users' data were collected in the context of ordinary arms-length commercial transactions between buyers and sellers. In other cases, the collection of transaction data may well create a reasonable expectation of privacy: consider the position of consumers who purchase medicaments, legal services or pornography online. Second, unlike *Golden Eye*, very few innocent users would be affected, since sellers were invariably in breach of the same ticketing conditions. This is unlike an application for bulk disclosure against an ISP, where a substantial percentage of affected subscribers may not be infringers. Both factors suggest that the approach taken in *Viagogo* is too simplistic and may not be readily adaptable to cases involving greater spill-over effects or data sensitivity.

Courts also assume that privacy interests are not engaged in respect of material known to breach a website's policies or terms of service.[234] That is to say, only posters of *permitted* material

---

[233] Michael Vogel, 'Unmasking "John Doe" Defendants: The Case against Excessive Hand-wringing over Legal Standards' (2004) 83 *Oregon Law Review* 795, 821.

[234] See, eg, *Sheffield*; *Clift*; *Viagogo (CA)*.

may reasonably expect privacy. There are three problems with this approach. The first is that even impermissible material may be legitimate and non-tortious. Users might expect that such material would be deleted, but not that it could justify disclosure to a third party who had no legal rights against its author. Second, courts do not consider whether a website's terms of use are reasonable. It is conceivable that the restrictions imposed may be so oppressive that they would fail to offer any guidance about what can legitimately be expected.[235] Third, it is doubtful whether consulting the terms of use will shed much light on the expectations of users — who rarely read or understand them.[236] In practice, most websites adopt terms which permit (and often make discretionary) disclosure of data in extremely broad circumstances. Consumers are rarely in a position to negotiate these terms. The courts' approach therefore has the unintended effect of encouraging intermediaries unilaterally to 'opt-out' from privacy protections.

(f) *Less intrusive alternatives to disclosure*

In weighing the proportionality of disclosure, one important consideration is whether an alternative procedure is available which poses a less substantial interference. Two alternatives to *Norwich Pharmacal* disclosure warrant consideration.

(i) *Litigation against persons unknown*

This first alternative is the service of John Doe proceedings, whereby permission is obtained under the applicable rules of court to effect alternate service by publishing or sending the claim form to the internet location where the original wrong is alleged to have taken place. Proceedings may then be commenced against 'persons unknown'.[237] Only after a full hearing would the Court unmask the defendant if the claimant has succeeded in obtaining a remedy. This neatly avoids the problem of excessive disclosure and, in some cases, may be a more proportionate way to ensure access to justice. However, such a procedure has some significant drawbacks. First, it may not always be possible to give the defendant effective notice of the proceedings. Second, even once notified, it may be difficult to evaluate the defendant's evidence unless they are willing to identify themselves privately to the Court. Finally, it may seem overly harsh to claimants to make them

---

[235] In *Viagogo (SC)*, Lord Kerr JSC accepted in *obiter* that ordinary consent extends, by necessary implication, only to lawful, proportionate disclosures, but did not consider the effect of a more extreme policy: at 3348.

[236] See Rebecca Smithers, 'Terms and Conditions: Not Reading the Small Print Can Mean Big Problems' (*The Guardian*, 11 May 2011) <http://guardian.co.uk/money/2011/may/11/terms-conditions-small-print-big-problems> (survey showing 7 per cent of UK internet users read terms and conditions before joining online services).

[237] See, eg, *AMP v Persons Unknown* [2011] EWHC 3454 (TCC) (ordering unknown file-sharers in possession of private images depicting the claimant to cease dealing with them).

invest resources to bring a claim without knowing the solvency of the defendant, which may affect the decision to sue. Accordingly, in most cases this is not a viable alternative to disclosure.

(ii) *Warning letters*

Another solution, modelled on the *DEA*, is to require intermediaries to forward notices detailing the claimant's allegations to the primary wrongdoer without disclosing their identity to the claimant. Claimants would be able to obtain de-anonymised subscriber data only where it can be shown that the tort is repeated or ongoing.[238] Further action may not be necessary if notices dissuade their recipients to renounce their tortious activity — though empirical evidence is divided on whether notices will have this effect.[239] Graduated response of this kind is clearly inappropriate for wrongs which may not occur more than once or require immediate relief, such as defamation or breach of confidence. However, in cases involving repeated or ongoing wrongs of a small scale, notification by the ISP may be a more proportionate response than disclosure, having regard to the relative impact on claimant and intended defendant. If the defendant heeds the notice and ceases wrongdoing, there would be no substantial purpose served by disclosure. If the wrongs continue (or are highly likely to do so), then disclosure may be necessary.

For copyright claims, the *DEA* creates a statutory right to disclosure. However, neither the Act nor the *Code* specify how applications for disclosure are to be determined: there must simply be 'an appropriate court order'.[240] Leaving aside the nebulous drafting, such an approach poses serious difficulties: the Act makes no provision for dealing with sensitive or personal information revealed on infringer lists; there is nothing to restrict the use of disclosed data or to require that disclosure be sought for a legitimate purpose. These omissions support the view that Parliament must have intended existing equitable principles to limit statutory disclosure. Certainly, the Act does not evidence an intention to make disclosure of unredacted infringer lists automatic — otherwise there would be no need for a court hearing.

4.4 Limitations upon disclosure

This section identifies five additional safeguards which it is suggested might better protect the rights of third party data subjects without reducing the utility of disclosure for claimants.

---

[238] See above chapter 5, § 3.1(b)(i).

[239] See above chapter 5, nn 183–190 and accompanying text.

[240] OFCOM, *Code*, §6.4.

(a) *Notice to the affected party*

In *Totalise*, Aldous LJ identified one of the less attractive features of *Norwich Pharmacal* relief: proceedings are *ex parte* as regards the user about whom disclosure is sought from the defendant. This means that the person most affected by disclosure has no ability to oppose it. In his place stands the intermediary, whose professed neutrality makes it a miserly champion — one that desires only to escape the proceedings without excessive expense or damage to its reputation. The Court is thus left to determine

> a contest between two parties, neither of whom is the person most concerned, the [third party] data subject; one of whom is the data subject's prospective antagonist; and the other of whom … would like to get out of the cross-fire as rapidly and as cheaply as possible. However, the website operator can, where appropriate, tell the user what is going on and to offer to pass on in writing to the claimant and the court any worthwhile reason the user wants to put forward for not having his or her identity disclosed. *Further, the court could require that to be done before making an order.*[241]

Although the courts in *Totalise*, *Sheffield* and *Golden Eye* ultimately did not require notice to be given, a notification requirement has much to commend it. Notice ensures that purported wrongdoers are aware of the allegations being made against them and given an opportunity to respond before an irreversible step is taken. This may result in the Court uncovering gaps in the evidence or other legitimate reasons why a third party stands to be disproportionately harmed by disclosure. This reduces the risk of error and better protects the affected parties' privacy. Indeed, data controllers are obliged under the first data protection principle to give notice to data subjects where practicable.[242] It is suggested that taking reasonable steps to notify should, where practicable, be a precondition of relief. Once notified, a third party could choose whether to tender a sworn statement to the Court on terms of confidentiality or make unsworn electronic submissions which could be taken into account. Without a procedural mechanism of this kind, third parties will be unfairly excluded from the process.[243]

Notification could not be absolute. Sometimes it may simply be impossible for the intermediary to contact the alleged wrongdoer. In such cases, notice might be attempted by analogy with the principles governing substituted service: for example, by posting a message to any associated website or forum.[244] Alternatively, there are good reasons to allow any interested

---

[241] *Totalise*, 1240 (Aldous LJ).

[242] *R (Ali) v Minister for the Cabinet Office* [2012] EWHC 1943 (Admin), [74] (Beatson J). See *DPA* sch 1, pt 2, para 2(3)(d).

[243] Smith, above n 4, 447.

[244] Cheverud, above n 207, 350.

party to oppose disclosure as *amicus curiae*, as occurred in *Golden Eye*.[245] This allows *amici* (most commonly consumer and civil liberties groups) to stand in for the affected parties to defend substantial or novel claims for disclosure, subject to bearing their own costs. Similar principles have been applied in *Anton Piller* applications with some success.[246]

Notification would also be inappropriate if a serious risk of prejudice could be shown by the applicant or if the number of affected parties is so large that individual notification would be unduly costly — though the cost of emailing even large numbers of customers can be overstated. This was the reason given in *Golden Eye*, along with the unlikelihood that many would respond.[247] In *Wikimedia*, Tugendhat J seems to imply that some cases may even require ancillary orders to prohibit disclosure of the fact that a *Norwich Pharmacal* order has been made.[248] Such a 'super-disclosure' order could only be justified in limited circumstances; for example, to prevent tipping off unidentified wrongdoers, who might take retaliatory steps or erase their tracks by requesting removal of all personal information held by any downstream service provider who could identify them.[249]

Against a notification requirement, two main objections may be raised. First, it might add unnecessary delay and expense. It is suggested that this risk is illusory: most obviously, courts could set strict timetables for third party submissions, consistent with the overriding objective. As to added expense, the answer is that such costs are not necessarily shouldered by the claimant, but by the party who emerges unsuccessfully from the ultimate proceeding. If anything, a notification requirement would reduce litigation costs by ensuring that claimants with unmeritorious claims are not able to get disclosure.

The second objection is that notification is unnecessary, since the Court is capable of carrying out the balancing exercise without assistance from the third party. The difficulty with this argument is that *Norwich Pharmacal* applications 'are not truly ordinary adversarial proceedings';[250] the presence of two litigants before the Court only distracts from what is, in substance, an *ex parte* procedure.[251] It is intrinsically difficult to ascertain the privacy interests of

---

[245] *Golden Eye*, [9] (Arnold J).

[246] *Ex parte Island Records Ltd* [1978] Ch 122, 133 (Lord Denning MR) ('invaluable').

[247] See, eg, *Golden Eye*, [140] (Arnold J) (notification of 9124 intended defendants refused).

[248] *Wikimedia*, [44].

[249] *DPA* s 7(1). See also Data Protection Principle 5.

[250] *Totalise*, 1239 (Aldous LJ).

[251] Although *Norwich Pharmacal* disclosure is technically a final 'remedy', it may not engage art 6 if it is treated, in substance, as an interim order: *X v United Kingdom* (1981) 24 DR 57 . See also Adrian Zuckerman, *Zuckerman on*

unrepresented and anonymous internet users, and impossible to predict possible reprisals and wider consequences of disclosure for their familial, vocational and personal relationships. Notification would mirror accepted practice in other jurisdictions.[252] It permits data subjects to contribute usefully to the delicate balancing of interests that is required under articles 8 and 10 — an inquiry which, as experience has shown, courts frequently get wrong even with the assistance of both affected parties. Notification may not solve the difficulties inherent in this exercise, but it would bring more of the relevant facts before the Court.

(b) *Cross-undertaking as to damages*

The authorities offer little recourse to parties who are adversely affected by disclosure that was wrongly given. Once disclosed, the secrecy of a party's identity cannot be restored[253] and even a triumphant defendant may face repercussions from employers, spouses, the press or the general public — without having committed any actionable wrong.[254] The lack of any mechanism to permit recovery of these losses from the claimant means there are limited disincentives against speculative applications. In appropriate cases, courts should therefore consider requiring the claimant to undertake to compensate the third party data subjects for any damage caused as a result of unwarranted disclosure.

Such an approach has two clear benefits. First, it would deter unmeritorious applications while still protecting the claimant's interest in borderline cases by allowing disclosure subject to the undertaking. Second, it ensures that *Norwich Pharmacal* orders cannot be abused by litigants to harass or embarrass anonymous internet authors without pursuing the primary claim. A cross-undertaking does not require any new head of liability; it is simply a condition of the Court agreeing to intervene in the *status quo* and grant injunctive relief in uncertain circumstances.[255]

Civil Procedure: Principles of Practice (2nd ed, 2006) 58 (suggesting that art 6 rights may not be engaged where the hearing does not determine the substantive dispute).

[252] See *Dendrite International Inc v John Doe No 3*, 775 A 2d 756 (NJ App Div, 2001) (requiring notice to be given to a third party, and an opportunity to make submissions before disclosure). In Canada, notice is optional: *BMG Canada*; *York University v Bell Canada Enterprises* [2009] CanLII 46447 (Unreported, ON SC, 4 August 2009) [24] (Strathy J).

[253] An affected party may, of course, take steps to conceal their online identity in the future, but, once revealed by disclosure, their association with past activities cannot easily be severed.

[254] Although it might be argued that the successful *Norwich Pharmacal* applicant owes a duty of care at least to the extent of keeping disclosed data secure, it is doubtful, in light of *Barclays Bank*, whether a cause of action could be sustained simply for non-compliance with the order's terms.

[255] See, eg, *Golden Eye*, [144] (Arnold J) (requiring an undertaking to sue in a particular court).

(c) *Full and frank disclosure*

Because intermediaries tend to take a neutral stance in disclosure proceedings, the Court must rely on information that is put before it by the applicant to make factual assumptions which may, after full evidence and argument, turn out to be incorrect, or which are never finally determined at trial.[256] In ordinary *inter partes* applications, the Court must be 'as satisfied as it can be having regard to the limitations which an interlocutory process imposes' that the claimant has 'a much better argument than the defendant.'[257] However, as discussed above, *Norwich Pharmacal* hearings more closely resemble *ex parte* applications, where the risk of unreliable decisions is compounded by the absence of the party most strongly affected.[258]

A sensible limitation is therefore to subject claimants to a duty of full and frank disclosure, just as applicants owe in *ex parte* procedures. The principles expressed in *R v Kensington Income Tax Commissioners; ex parte de Polignac* apply wherever an application is made 'in the absence of the person who will be affected by that which the court is asked to do'.[259] Because the users affected by disclosure are rarely represented at *Norwich Pharmacal* hearings, it follows that the applicant should owe such a duty. This 'ingenious argument' was considered but not resolved by Arnold J in *Golden Eye*,[260] since breach of any duty could only be determined once disclosure had already been ordered.[261] The difficulty with this reasoning is that, by the time an affected subscriber is in a position to make such an application, the damage will already have been done, since their anonymity cannot be restored. A clear statement of principle is needed in advance of disclosure to encourage applicants to act with *uberrimae fidei*.

(d) *Supervision orders*

Because the applicant is not obliged to commence proceedings and so have the issues finally determined, the Court has limited ability to control use of the information once disclosed. One solution is to require judicial or other independent supervision of the execution of the orders; for example, by appointing a neutral solicitor, by analogy with *Anton Piller* search orders. A similar suggestion was made by HHJ Birss QC in *Media CAT*,[262] but rejected in *Golden Eye*. Arnold J

---

256 Hew Dundas, 'Russian Billionaires Revisit *Norwich Pharmacal* Orders' (2011) 77 *Arbitration* 362, 363.

257 *Bols Distilleries BV v Superior Yacht Services Ltd* [2007] 1 WLR 12, 22 (Lord Rodger).

258 See *Media CAT [No 2]*, [14] (HHJ Birss QC).

259 [1917] 1 KB 486, 509 (Warrington LJ).

260 *Golden Eye*, [88] (Arnold J) (while a failure to adduce relevant evidence may lead to adverse inferences being drawn against the applicant, this was independent of any duty).

261 Ibid [86]–[88] (Arnold J).

262 *Media CAT*, [112] (HHJ Birss QC).

concluded that a supervisor would lack binding authority over the third parties and could not function as a useful arbiter of disputes. However, a neutral observer could play various other roles; in particular, monitoring settlement correspondence between the claimant and third parties, and auditing the storage security of disclosed data. While supervision may seem heavy-handed, in the absence of any other meaningful limitation on post-disclosure conduct, it could offer a useful safety-net against misuse — particularly where the scale of disclosure is substantial or the information is sensitive.[263]

(e) *Implied undertaking*

Use of disclosed information should be restricted to the purpose of taking action against the identified parties or ultimate wrongdoer. That is the basis for intruding upon the privacy of the alleged wrongdoer; if it eventuates that no tort has been committed by them or any related party against the applicant, it seems unjustifiable to allow that information to be retained or used for any other purpose. This limitation follows by analogy with the restrictions on information obtained under regular civil disclosure,[264] which prohibit use for any 'collateral or ulterior purpose'.[265] Identity disclosure involves the same principle of public policy — namely, that the fruits of a compulsory and intrusive legal procedure should not be given over to the unconditional use of the claimant. This limitation discourages fishing expeditions and ensures respect for the rights of data subjects. Alternatively, disclosed information could be given an 'expiry date' by which the applicant must have commenced proceedings (or taken whatever legitimate action was pleaded) or otherwise undertake to destroy it.

In appropriate cases, the Court should also issue specific directions, such as anonymity orders, limiting how the disclosed data may be accessed and used,[266] and requiring the disclosing and receiving parties to encrypt personal data securely. In failing to impose such requirements, courts are contravening the seventh Data Protection Principle, which requires appropriate technical measures to be taken to prevent unlawful processing of personal data. The consequences of unencrypted disclosure can be serious for internet users. In *Media CAT*, the original order

---

[263] Alternatively, a return date could be specified on which the applicant must return to obtain directions after the information has been disclosed, or to account for the use he has made of the information. At this point, group litigation orders could be made in appropriate cases under *Civil Procedure Rules* pt 19, or the original orders for disclosure varied if necessary: see *County Courts Act 1984* (UK) s 38(1); *County Court Remedies Regulations 1991* (UK) [2]–[3]; *Senior Courts Act 1981* (UK) s 15(3)(b).

[264] See *Home Office v Harman* [1983] AC 280.

[265] See also *Civil Procedure Rules* pt 31.22.

[266] *BMG Canada*, [43]–[45] (Sexton JA).

required password-protection of the disclosed data. However, contrary to the order, BT and several other ISPs sent their data in plain text or weakly-protected spreadsheets.[267] In May 2010 an unsecured email server belonging to the claimants' solicitors was attacked by vigilante activists.[268] Somewhat ironically, the spreadsheets disclosed by the ISPs propagated rapidly on P2P networks and cyber-lockers. Many subscribers (even those who had settled claims) were publicly identified. This regrettable coda to the *Media CAT* saga could have been avoided had data encryption requirements formed a clearer element of the disclosure obligations.

4.5 Liability for costs

The allocation of costs can be of decisive importance, since intermediaries are even less likely to oppose disclosure if they risk a costs penalty for doing so. The current approach to assessing costs generally reflects the fact that the order is made against an innocent party, but its application to internet intermediaries has become progressively more unclear, leading fewer intermediaries to contest disclosure.

(a) *The general rule*

The exercise of the protective jurisdiction — of which *Norwich Pharmacal* orders are but one example — against otherwise blameless conduits or custodians should entitle the intermediary to all their costs and expenses. This has not always been so. In *Upmann v Elkan*, the trial judge found for the plaintiff and ordered disclosure, but made no order as to costs,[269] meaning that the forwarding agents were required to bear all costs of disclosure and ongoing monitoring of future cigar shipments. This position was effectively reversed in *Norwich Pharmacal*, where Lord Reid commented that the defendant should ordinarily be reimbursed for the cost of contesting disclosure, it being desirable to have the issue determined judicially:[270]

---

[267] Elsevier Ltd, 'BT Admits Passing Unencrypted Customer Data to ACS:Law' (*Info Security Magazine*, 30 September 2010) <http://www.infosecurity-magazine.com/view/12865/bt-admits-passing-unencrypted-customer-data-to-acslaw/>.

[268] John Leyden, 'Anti-Piracy Lawyers' Email Database Leaked after Hack' (27 September 2010) *The Register* <http://www.theregister.co.uk/2010/09/27/anti_piracy_lawyer_email_leak/>.

[269] *Upmann v Elkan*, 148 (Romilly MR).

[270] *Norwich Pharmacal*, 175 (Lord Reid).

> If the respondents have any doubts in any future case about the propriety of making disclosures they are well entitled to require the matter to be submitted to the court *at the expense of the person seeking the disclosure.* The court will then only order discovery if satisfied that there is no substantial chance of injustice being done.[271]

Lord Cross stated that, in all but the simplest of cases, the respondent would be justified in asking the Court to rule on the availability of disclosure. The Court would then require the applicant to bear '[t]he full costs of the … application and any expense incurred in providing the information'.[272]

In this respect, proceedings under the equitable protective jurisdiction differ from normal proceedings where the costs of the successful party are ordinarily paid by the unsuccessful party. This reflects the historical basis of the jurisdiction — a non-party named in a bill of discovery was entitled to recover costs[273] — and the policy that costs be paid not by an innocent party but by the unsuccessful party, as Aldous LJ commented in *Totalise*.[274] While there are exceptions to this principle, most intermediaries will be entitled to resist a request for disclosure and have their costs. For example, in *Smith, Kline and French Laboratories Ltd v R D Harbottle (Mercantile) Ltd*,[275] British Airways carried a patented medicament on consignment for the other defendants. The claimants obtained an injunction prohibiting delivery. The Court likened the airline's position to a 'mere carrier' or warehouseman and held that, as an innocent non-infringer, British Airways was entitled to payment of its costs and carriage expenses.[276]

(b) *Application to internet intermediaries*

Whether or not the defendant is an internet intermediary or another innocent party should not affect their liability for costs. As Aldous LJ held in *Totalise*:

> the defendant, whether it be a web provider, Customs and Excise, a telephone company or a bank, does not normally resist the order being made. Such defendants have become mixed up in tortious acts and are only

---

[271] Ibid 176 (Lord Reid) (emphasis added).

[272] Ibid 199 (Lord Cross).

[273] See *Beames on Costs* (2nd ed, 1840) § IV, 17; *Bray on Discovery* (1885) 618; cited in *Norwich Pharmacal*, 154.

[274] *Totalise (CA)*, [29]–[30].

[275] [1980] RPC 363.

[276] Ibid 367–8, 374 (Oliver J).

> concerned that duties and rights … are considered by the court. It is for the applicant to satisfy the court that the order should be made, not for the defendant to take a view which could be wrong.[277]

Totalise is considered the modern authority on costs in *Norwich Pharmacal* applications. There the respondent website operator ('Interactive') initially refused disclosure but adopted a 'purely neutral' position at trial.[278] The trial judge considered that it was wrong for Interactive to oppose the order and awarded costs against it. Appealing on the issue of costs, Interactive successfully argued that an adverse costs order should not be made where an intermediary: reasonably and genuinely doubted its obligation to disclose the information; faced liability or other damage if voluntary disclosure was given; or could identify a third party's legitimate interest which disclosure *might* infringe.[279]

By analogy with the rules governing pre-action disclosure, Aldous LJ held that generally, costs incurred should be recovered from the primary tortfeasor rather than from an innocent party such as an intermediary. Only where the respondent is 'implicated in a crime or tort or seeks to obstruct justice being done' should it be required to bear its costs. There being legitimate doubts about Interactive's obligation to give disclosure and the weight to be accorded to the anonymous author's privacy, costs were awarded against the claimant. However, given that future applications will presumably carry greater legal certainty, the default position remains somewhat unclear.

An innocent intermediary should not be penalised for having the claimant's allegations tested. This is consistent with the view that equitable disclosure imposes only a procedural liability: to require an innocent party to bear a financial burden in giving disclosure would, in the absence of wrongdoing by them, be improper. This approach carries several important benefits. First, it deters unmeritorious applications. Second, intermediaries are likely to take greater care in identifying the correct records if they know they will be reimbursed for the trouble. Third, the Court may be able to offset any additional costs to the applicant by consolidating related actions — as occurred in *Media CAT* — or by sensibly confining the scope of disclosure. The compliance costs of giving disclosure are not likely to be high: one search engine estimates its cost at around £30 per record of information sought.[280] The costs of the hearing are likely to be far greater.

Finally, shielding intermediaries from adverse costs orders encourages judicial determination of disclosure claims and reduces pressure on self-interested intermediaries to give

---

[277] *Totalise (CA)*, 1239 (Aldous LJ).

[278] Ibid 1235 (Aldous LJ).

[279] Ibid 1237 (Aldous LJ).

[280] Interview, Jenni Aldrich, Regional Legal Director, Google Australia Pty Ltd (19 December 2011, Sydney).

voluntary disclosure. Private ordering is undesirable because it would be neither more efficient nor reliable than court-mediated disclosure. It would not appreciably reduce compliance costs because the same records would still need to be disclosed. Further, it would leave difficult questions of public policy undetermined and relegate decisions affecting numerous individuals to private entities who have limited incentives to take fundamental rights into account. Private capitulation leaves the primary claims untested and conceals the manner in which the information was obtained. A costs rule which more strongly incentivises judicial supervision is therefore desirable.[281] More fundamentally, it reflects the important policy that innocent parties should not be liable to pay costs.

5 Conclusion

Disclosure plays an increasingly vital role in regulating the liability of internet intermediaries. It justifies and complements the broad limitations upon their monetary liability by assisting claimants to obtain meaningful relief against primary wrongdoers, and recognises that many facilitators occupy an indeterminate space between culpability and neutrality. The application of traditional equitable principles to internet intermediaries illustrates their flexibility and reflects the wider shift from monetary remedies to injunctive and other non-monetary relief. Where claimants once sought to hold intermediaries secondarily responsible for misconduct, disclosure orders provide a mechanism for regulating intermediaries' activities without alleging fault. This is attractive to claimants because it allows them to sidestep the safe-harbour regime and enforce their rights directly against primary wrongdoers. This both deters tortious conduct and enforces primary norms, thereby upholding the rule of law without imposing an unreasonable enforcement burden upon intermediaries. When combined with the new injunctive remedies considered in the next chapter, it provides a strong foundation for pursuing internet tortfeasors in a fair, efficient and proportionate way.

Although flexible and effective, disclosure suffers from several major defects. First, the procedure does not scale particularly well, and use of material obtained by disclosure is inevitably limited by the commercial reality that, in many cases involving allegations of widespread but minor wrongdoing, it will be uneconomic to proceed against every identified tortfeasor. Second, the effects of disclosure can be tantamount to the grant of an *ex parte* substantive remedy, but procedurally it is treated as if it were an ordinary *inter partes* proceeding. In some cases, the very

[281] See Suzor, above n 221, 266.

threat of disclosure may induce the putative wrongdoer to cease the relevant activity or withdraw the offending content, whether or not tortious. This encourages over-compliance and carries spill-over costs.

Third, the elements of *Norwich Pharmacal* relief are inherently claimant-friendly and their application to internet intermediaries accentuates that imbalance. The low threshold of facilitation means that almost any dealing by an intermediary will be sufficient. While proportionality offers constructive tools with which to balance the competing interests, the scales remain tipped too far in favour of claimants. Intermediaries face adverse costs orders if they oppose an application too strenuously, while affected users lack notice of the application and cannot make submissions defending their own interests until after their anonymity has already been irreversibly destroyed. Cases such as *Media CAT* remind us of the risk that disclosure remedies will ultimately be misused by litigants. In many cases, users are treated as if they were proven wrongdoers when there is likely to be an appreciable proportion of innocent people affected by disclosure. Although that proportion will be higher in some cases (*Golden Eye*) than others (*Viagogo*), the privacy analysis has a tendency to elevate allegation into certainty.

Some encouragement may be taken from the detailed analysis of users' rights seen in cases like *Golden Eye*. However, further safeguards are needed to guide the application of the equitable jurisdiction to internet intermediaries. To a large extent, *Norwich Pharmacal* jurisprudence can be understood as an attempt to define limits on the Court's power to interfere with the affairs of innocent parties. Where the precise limits lie is a matter for individual cases, but default rules are important where there is a risk of imperfect representation. Because neither party appearing before the Court has the necessary incentive to represent the public interest, there is a real danger that disclosure will not do justice if third parties' rights are sacrificed on the altar of expedience.

This chapter has defended *Norwich Pharmacal* disclosure while offering several procedural reforms. Adopting these recommendations would go a long way towards restoring balance and proportionality to their use against internet intermediaries. Like many questions of internet policy, the balance is a delicate one and many competing interests are implicated. The adoption of sector-specific regulatory schemes (as in the case of copyright and ISPs) may reduce the cost of enforcement, but leaves crucial questions of disclosure policy to the courts. Disclosure should continue to uphold the rights of claimants to vindicate internet wrongdoing against them and to compel intermediaries to assist in identifying a proper defendant. However, courts must be vigilant in requiring sufficient proof of wrongdoing, restricting the scope, purposes and subjects of disclosure, and limiting the grant of disclosure in appropriate ways. Privacy and freedom of

expression are not necessarily inconsistent with claimants' rights, but care must be taken to ensure that both sets of interests are fully recognised.

In chapter 7, these proposed reforms are integrated into a wider framework of injunctive remedies against intermediaries. The wrongs considered in chapters 4 and 5 are re-examined and it is argued that clearer exclusions of intermediaries' monetary liability are justified by the availability of three new forms of injunctive relief under the equitable protective jurisdiction: blocking, de-indexing and asset freezing orders.

7
Non-facilitation

A person harmed by tortious material on the internet can seek to enforce their rights against intermediaries using three remedies. The first is well-known and has been discussed in chapters 4 and 5: the material can be removed at its source, either by sending a sufficient notice to the intermediary or, if it fails to act expeditiously, by way of mandatory injunction or an action claiming damages. Chapter 6 identified a second, complementary mechanism: an intermediary may be ordered to disclose the primary tortfeasor's identity, opening the path to a direct remedy. These remedies will often prove unsatisfactory because of difficulty pursuing the primary tortfeasor or securing the cooperation of an intransigent extraterritorial intermediary. To respond to these situations, this chapter proposes a third set of non-monetary remedies designed to make it more difficult for internet users located within the jurisdiction to *access* material which cannot be removed by other means. In particular, it advocates the recognition of blocking injunctions, which order ISPs to adopt technical measures aimed at filtering specific content, and de-indexing injunctions, which order search engines and other gateways to disable hyperlinks to a precisely specified internet location. It also advocates the extension of asset freezing orders to payment intermediaries. Section 1 sketches the elements of a general non-facilitation injunction to impede access to tortious internet material in a proportionate manner, which is founded upon

the equitable protective jurisdiction. Section 2 discusses the three proposed orders, their potential effectiveness and proper limits.

1 Equitable non-facilitation orders

This section proposes a general remedy to order a non-infringer to cease facilitating a third party's primary wrongdoing where it is necessary and proportionate to do so. Properly understood, this is not a radical change in the law but simply an expression of the wider principle underlying *Norwich Pharmacal* orders and the equitable protective jurisdiction; namely, that a secondary actor who becomes mixed up in primary wrongdoing owes a duty not to continue facilitating that wrongdoing once notified of its existence. When understood in light of *Convention* jurisprudence and European law, equity requires such intermediaries to act so as to preserve the claimant's primary rights where no viable alternative exists for their protection. These parties are not mere witnesses, since they knowingly facilitate wrongdoing. Like disclosure, the defendant need not have committed any tort. It imposes no monetary liability and ordinarily requires the claimant to pay the defendant's reasonable enforcement costs. It is simply a mandatory injunction[1] sought on notice to the defendant and usually to the primary wrongdoer. It is, of course, not limited to internet wrongdoing — such an order could be sought against a bank, carrier, warehouseman or any other offline intermediary — though this chapter examines and defends the remedy in that context. This section begins by identifying, first, the jurisdictional basis of the remedy and, second, its constituent elements.

1.1 Jurisdictional basis

In addition to tort-specific statutory remedies,[2] English courts have an inherent jurisdiction to grant injunctions wherever it is just and convenient to do so.[3] This is a jurisdiction of almost unlimited breadth and flexibility,[4] which suggests that it could be used to fashion a non-facilitation remedy in limited circumstances against non-tortfeasor intermediaries. Although this is an

---

1 Although non-facilitation orders may be framed negatively — eg, as a prohibitory injunction requiring an ISP *not* to facilitate access to a specified internet location —their substance is *mandatory*: they create positive obligations to withdraw the support (eg, by blocking or disabling access) which intermediaries ordinarily give: see *Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289, 394 (Laddie J) ('*Ocular Sciences*').

2 See, eg, *Copyright Act* s 97A; see below § 2.1.

3 See *Senior Courts Act 1981* (UK) s 37(1); *County Courts Act 1984* (UK) s 38(1).

4 See Zuckerman, above n 251 (ch 6), 299–301 (interim injunctions). See, eg, *Dyson Appliances Ltd v Hoover Ltd [No 2]* [2001] RPC 27 (fashioning an anti-springboarding injunction following patent infringement).

attractive option which would not require statutory implementation, such an argument faces considerable — but, it will be suggested, not insurmountable — difficulties.

(a) *Equitable injunctions*

At the outset, we must take care to distinguish among several sources of power to grant injunctive relief. The grant of an injunction in aid of legal or equitable rights involves the equitable *auxiliary* or *exclusive* jurisdiction, respectively.[5] Similarly, the equitable *protective* jurisdiction preserves the claimant's ability to assert or enforce her rights in a subsequent trial against the primary wrongdoer; for example, by requiring the disclosure or preservation of evidence.[6] In all cases the claimant must show some right which is or is at risk of being infringed, normally by the defendant to the action.

Where a recognised right has been infringed and the defendant has no countervailing interest or defence, the claimant is '*prima facie* entitled to an injunction'.[7] Such orders operate *in personam* and will not normally bind non-parties.[8] Relief is still traditionally refused in three situations: first, if a substitutive remedy such as damages (or, in the case of an equitable wrong,[9] equitable compensation) would prove adequate, or if an injunction would cause disproportionate harm to the defendant;[10] second, if the claimant is guilty of delay, acquiescence or other misconduct which makes equitable relief inappropriate;[11] and third, if to grant an injunction would be futile.[12] These general limitations would apply to claims for non-facilitation remedies.

(b) *Injunctions without wrongdoing*

A non-facilitation remedy requires proof of at least *prima facie* wrongdoing. However, that wrong need not be committed by the respondent to the order. There are cases in which — for reasons of practical or commercial necessity, procedural fairness or the protection of fundamental rights — injunctive relief is available against a party who has committed no legal or equitable wrong against

---

5 *Vestergaard Frandsen A/S v BestNet Europe Ltd* [2010] FSR 2, 43–4 (Arnold J).

6 *Norwich Pharmacal*, 145 (Buckley LJ), 175 (Lord Reid); *Interbrew*, 457 (Sedley LJ).

7 *Shelfer v City of London Electric Lighting Co [No 1]* [1895] 1 Ch 287, 322 (Smith LJ).

8 *Iveson v Harris* (1802) 7 Ves Jun 251, 256–7 (Lord Eldon).

9 See R P Meagher, J D Heydon and M J Leeming, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (6th ed, 2006) [41-135].

10 See *National Provincial Plate Glass Insurance Co v Prudential Assurance Co* (1877) LR 6 Ch D 757, 761 (Jessel MR), 769 (Fry J).

11 *Hubbard v Vosper* [1972] 2 QB 84, 96–7 (Lord Denning MR).

12 See *Northern Rock plc v Financial Times Ltd* [2007] EWHC 2677 (QB).

the claimant. In these cases, injunctive relief does not rest upon any tortious conduct *by the defendant* but is instead founded upon, variously, a recognised causal relationship between the defendant and a third party tortfeasor, the *parens patriae* (wardship) jurisdiction,[13] the need for Courts to act compatibly with human rights, or the receipt of notice of an injunction against a third party. Equitable relief in these cases does not require proof of actual or threatened wrongdoing; it 'floats' upon the Court's inherent jurisdiction to uphold the administration of justice and thereby binds the respondent.

At least six instances of these 'floating' injunctions may be identified. First, a *Mareva* injunction obliges an innocent party (typically a financial institution) to prevent the dissipation of assets,[14] notwithstanding that dissipation by the respondent may not amount to a tort. Second, a *Norwich Pharmacal* injunction obliges disclosure and, as discussed in chapter 6, proceeds on the basis that the respondent is not a tortfeasor but rather a *facilitator* of wrongdoing.[15] Third, an *Anton Piller* injunction obliges a party to preserve and grant inspection of relevant evidence that would otherwise face a serious risk of destruction.[16] Such orders proceed from paramount necessity to preserve other rights belonging to the applicant, but the respondent need not have committed or be proposing to commit any tort.[17] Fourth, the High Court can grant relief in aid of litigation abroad, even where no wrongdoing is alleged in the United Kingdom.[18] Fifth, a defendant may be restrained from activity likely to lead to future wrongs, even if its prior conduct is not tortious.[19]

Finally, the *Spycatcher* principle allows an injunction to be made *contra mundum* in an action against a primary wrongdoer and so bind any party having notice of it.[20] Notified parties are obliged not to do anything to undermine or assist a breach of the injunction, or face liability as

---

13 See *Wellesley v Duke of Beaufort* (1827) 2 Russ 1, 20 (Lord Eldon); *Scott v Scott* [1913] AC 417, 483 (Lord Shaw).

14 See below § 2.3; *Mareva*; *Civil Procedure Rules* r 25.1(1)(f).

15 *Norwich Pharmacal*, 175 (Lord Reid). See also *Bankers Trust Co v Shapira* [1980] 1 WLR 1274, 1282 (Lord Denning MR); *Aamer v The Secretary of State for Foreign and Commonwealth Affairs* [2009] EWHC 3316 (Admin), [43].

16 *Anton Piller KG v Manufacturing Processes* [1976] Ch 55 ('*Anton Piller*'). See now *Civil Procedure Act 1997* (UK) s 7; *Civil Procedure Rules* r 25.1(h).

17 *Lock International Corporation v Beswick* [1989] 1 WLR 1268, 1281 (Hoffmann J).

18 See *Civil Jurisdiction and Judgments Act 1982* (UK) s 25(1); *Civil Jurisdiction and Judgments Act 1982 (Interim Relief) Order 1997* (UK) [2]; Zuckerman, above n 251 (ch 6), 349.

19 See, eg, *British Data Management plc v Boxer Commercial Removals plc* [1996] 3 All ER 707 (injunction *quia timet*). In other contexts, see *Crime and Disorder Act 1998* (UK) s 1(1) (anti-social behaviour orders), 8A(2) (parenting orders); *Protection from Harassment Act 1997* (UK) s 5 (restraining orders).

20 See *Attorney–General v Newspaper Publishing plc* [1988] Ch 333, 375, 380 (Lloyd LJ); *Attorney General v Times Newspapers Ltd* [1992] 1 AC 191, 223–4.

contemnors.[21] This consequence makes *Spycatcher* orders an attractive remedy in cases involving privacy or confidential information, since the net of non-disclosure can be widely cast. The justification for such orders 'is now derived from *Convention* rights',[22] because s 37(1) must be read in conjunction with ss 3, 6(1) and 6(3)(a) of the *HRA*. The *contra mundum* jurisdiction has its basis in the protection of fundamental rights and requires the Court to undertake the familiar balancing exercise.[23] Realistically, this may cover most instances of defamation and copyright wrongs — the former engaging the claimant's article 8 rights, the latter article 1 of the First Protocol. It follows that, at least in cases where *Convention* rights are engaged, the Court may have power to grant a non-facilitation remedy if, on a proper assessment of the competing rights, it is necessary and proportionate to do so.

(c) *Injunctions under the 'broad' view*

If an intermediary has not engaged in wrongdoing and the case does not fall within a recognised category of floating injunction, it is uncertain whether it could be enjoined from assisting a tort. There are two possible approaches. According to the narrow view, an injunction, being a specific remedy, is granted only in aid of existing legal or equitable rights enjoyed against the party to be enjoined (subject to the limited exceptions noted previously). In *The Siskina*, Lord Diplock reasoned that to grant an interim injunction required 'a pre-existing cause of action *against the defendant* arising out of an invasion, actual or threatened by him, of a legal or equitable right of the plaintiff'.[24] This view finds support in a line of authorities going back to *North London Railway Co v Great Northern Railway Co*, where Cotton LJ held that the predecessor of s 37(1) required the existence of recognised category of right before the Court had jurisdiction to grant an injunction.[25]

According to the broad view, the statutory jurisdiction is not so constrained.[26] As Lord Nicholls argued in a dissenting speech in *Mercedez-Benz AG v Leiduck*:

---

[21] See *Jockey Club v Buffham* [2003] QB 642; *Hutcheson v Popdog Ltd* [2011] EWCA Civ 1580, [26]. However, while there is no authority on the point, it is open to doubt whether a failure successfully to restrict access could be regarded as sufficiently flouting the terms of the injunction to warrant a finding of contempt. A failure to block or de-index may indirectly assist a breach of the injunction, but it is not a positive or specific action in the same way as publishing an embargoed article.

[22] *In re S (a child)* [2005] 1 AC 593, [23] (Lord Steyn).

[23] *Attorney General's Reference No 3 of 1999: Application by the British Broadcasting Corporation to set aside or vary a Reporting Restriction Order* [2010] 1 AC 145, [52]–[57], [64]–[65] (Lord Brown) (Lord Phillips, Lord Hope and Lord Walker agreeing). See also *OPQ v BJM* [2011] EWHC 1059 (QB), [18]–[26] (Eady J).

[24] *Siskina (Owners of Cargo Lately Laden on Board) v Distos Compania Naviera SA* [1979] AC 210, 256 (Lord Diplock) (emphasis added) ('*The Siskina*').

[25] (1883) 11 QBD 30, 39–40 (Cotton LJ). See also *Mareva*, 510 (Lord Denning MR).

[26] See, eg, *Rasu Maritima SA v Perusahaan Pertambangan* [1978] QB 644; *A J Bekhor & Co Bilton* [1981] QB 923.

> the jurisdiction to grant an injunction, unfettered by statute, should not be rigidly confined to exclusive categories by judicial decision. The court may grant an injunction against a party properly before it where this is required to avoid injustice … The court habitually grants injunctions in respect of certain types of conduct. But that does not mean that the situations in which injunctions may be granted are now set in stone for all time.[27]

However, the majority expressly adopted the narrow view.[28] Even Lord Nicholls accepted that, before granting relief, the Court must be satisfied that there is a cause of action 'recognised by English law' and that the relief is ancillary to that action.[29] In the *Channel Tunnel* case Lord Mustill went further, requiring that an interlocutory injunction be 'always incidental to and dependant on the enforcement of a substantive right'.[30] This reflects the approach approved in *The Siskina*, where Lord Diplock characterised a *Mareva* injunction as ancillary to a substantive claim for debt or damages against the primary wrongdoer.[31] Although a complete review of the authorities is beyond the scope of this chapter, it seems clear that the narrow view reflects the preferred approach. Nevertheless, there are good arguments that a more flexible approach should apply; after all, many useful freestanding remedies — including *Mareva* orders and anti-suit injunctions — owe their existence to the continuous adaptation of s 37(1) to meet new circumstances. As Lord Scott remarked in *Fourie v Le Roux*, such remedies could not have developed 'if Cotton LJ's proposition still held good.'[32]

(d) *Equitable protective jurisdiction*

A final possibility is that non-facilitation orders could be fashioned within the equitable protective jurisdiction. By analogy with *Norwich Pharmacal*, a person who innocently facilitates tortious activity should owe a duty to co-operate in 'righting the wrong' by ceasing to facilitate further wrongdoing once notified of it. Thus, the wharfingers in *Orr* owed a duty not to part with goods they knew to be infringing, and the labellers in *John Walker* owed a duty not to supply inherently deceptive instruments which they knew would be used in wrongdoing.[33] So too, in *Silverlock* and *One in a Million*, an injunction issued to prohibit the defendants from facilitating passing off; while in *Intercen* there are good arguments that the airliner could have been enjoined from transporting

---

[27] [1996] AC 284, 309 ('*Mercedez-Benz*').

[28] *Mercedez-Benz* [1996] AC 284, 301 (Lord Mustill); cf ibid 307–8 (Lord Nicholls) (dissenting).

[29] See *Channel Tunnel Group Ltd v Balfour Beatty Construction Ltd* [1993] AC 334, 341 (Lord Browne-Wilkinson) ('*Channel Tunnel*').

[30] Ibid 362 (Lord Mustill).

[31] *Siskina*, 253 (Lord Diplock).

[32] [2007] 1 WLR 320, [30] (Lord Scott) ('*Fourie*').

[33] See above chapter 3, § 1.3(b)(iii); chapter 6, § 2.1.

the defendants' infringing goods. In *Upmann v Elkan*, just as important as disclosure was the dock company's obligation not to forward the counterfeit goods. These cases illustrate the jurisdiction's long-standing but largely forgotten potential to prohibit those mixed up in tortious acts from continuing to facilitate wrongdoing.

Similarly, it could be said, search engines and ISPs owe an equitable duty not to facilitate the continuation of wrongdoing by supplying transmission services or drawing attention to tortious material. Restricting access to tortious electronic publications is one important incident of this duty, but its content will vary depending on the nature of primary wrongdoing. Once material is proved to be tortious, an equitable occlusion duty should be enforceable by injunction if the facilitator is otherwise unwilling to act. In unwittingly facilitating access or directing users to tortious material, an intermediary may become sufficiently mixed up in the tort to justify injunctive relief to protect the claimant's rights, subject always to any countervailing interests. Unwitting assistance is, of course, insufficient for monetary liability in tort, but — as discussed in chapter 6 — it may create duties in equity which are enforceable by injunction.

This logic applies as readily to copyright torts as it does to other types of wrongdoing. If anything, the argument is strengthened by the obligation of courts to interpret s 37(1) compatibly with European law to the extent possible[34] — and specifically, article 8(3) of the Information Society Directive and articles 9 and 11 of the Enforcement Directive. Arnold J reached a similar conclusion in *eBay*, holding that s 37(1) may include the power to grant an injunction against an intermediary whose services had been used by third parties to infringe a registered trade mark, if that is what article 11 required.[35] Although this was not *acte clair*, the CJEU explained that article 11 does require an injunction which is effective, dissuasive and proportionate, and able to prevent future wrongdoing of the same kind. An appropriately framed non-facilitation order could meet this description. In *eBay*, the injunction would be to prevent the listing of specific products certified as counterfeit by the claimant, though this would be subject to the general limitations on monitoring duties, supervision and futility.

---

[34] See Case C-106/89, *Marleasing SA v La Comercial Internacional de Alimentación SA* [1990] ECR I-4135, 4159 ('*Marleasing*'); *Ghaidan v Godin-Mendoza* [2004] 2 AC 557, 572 (Lord Nicholls), 585–6 (Lord Millett), 596–8 (Lord Rodger).

[35] *eBay*, 185–6, 189 (Arnold J).

(e) *ACTA*

It is worth noting that *ACTA* requires English courts to possess the power to issue 'prompt and effective' interim and final injunctions to an infringer and, 'where appropriate, to a third party'.[36] *ACTA* does not confine the circumstances in which relief may be ordered by reference to any connecting factor. Instead, an intermediary may 'where appropriate' be ordered to prevent any infringement.[37] If, as argued above, English courts already possess the power to make such orders, transposing these provisions would not require drastic alterations to the existing tapestry of intellectual property remedies. However, the desirability of interpreting domestic instruments (such as s 37(1)) compatibly with international treaty obligations may mean that these provisions alter the calculus according to which the Court's discretion must be exercised.

(f) *Preliminary conclusions*

The foregoing discussion suggests three tentative conclusions. First, although there is no express statutory jurisdiction to grant non-facilitation injunctions, there are good arguments that s 37(1), read in conjunction with ss 3 and 6(1) of the *HRA*, confers sufficient jurisdiction for courts to grant relief where three conditions are satisfied: (1) the applicant's *Convention* rights are engaged; (2) on a proper balancing of the competing interests, the applicant's rights should prevail; and (3) the injunction is a necessary and proportionate measure to protect those rights. Second, in other cases, it is possible that an injunction could issue in one of three ways: (1) against the primary wrongdoer and then brought within the *Spycatcher* principle by service upon each intermediary sought to be enjoined; (2) in aid of rights in a proceeding being litigated abroad; or (3) as an order ancillary to a local claim against the primary wrongdoer, pursuant to the equitable protective jurisdiction. Third, in intellectual property claims an injunction may be available under s 37(1) interpreted compatibly with the Enforcement Directive and *ACTA*, provided that the order meets the requirements (of fairness, cost and proportionality) discussed in chapter 3.

1.2 Elements of relief

It is desirable to specify the contours of the remedy in a manner that ensures certainty, economy and safeguards against abuse. This section briefly outlines four elements of a possible non-

---

[36] *ACTA* arts 8.1, 12.1(a).

[37] *ACTA* arts 8.1, 12.1, 10.2.

facilitation remedy which, by analogy with *Norwich Pharmacal* orders, the Court should consider when determining whether to exercise its discretion in the claimant's favour. Alternatively, these elements could form the basis of a codified statutory remedy.

(a) *Wrongdoing*

The claimant must establish real prospects of succeeding in a claim for a substantial primary wrong which is causing appreciable actual or foreseeable harm. This is consistent with the heightened threshold suggested should apply to claims for *Norwich Pharmacal* relief, reflecting the general criteria for mandatory injunctions in contexts affecting freedom of expression.[38] Without demonstrating a likelihood of wrongdoing by *someone*, the court has no jurisdiction to enjoin an intermediary. As discussed in chapter 6, this determination of lawfulness should be made by a court rather than by algorithm or accusation. By analogy with the threshold requirements for defamation and disclosure, the wrongdoing must be substantial — sufficient to make the claim 'worth the candle' — and not trivial or minor. Like *Norwich Pharmacal*, an application could be founded in potentially any form of civil wrongdoing.

(b) *Facilitation*

The defendant must be shown to facilitate the primary wrongdoing. This may, for example, be by supplying communications facilities (ISPs), hyperlinks (search engines, websites) or payment gateways (marketplaces, transaction processors). Where the wrongdoing consists of publishing tortious material which is obscure, the applicant may be required to prove substantial access within the jurisdiction by analogy with the publication cases considered in chapter 4. The claimant would need to identify with precision the URLs, search queries or other mechanisms by which wrongdoing was facilitated. Like disclosure orders, the intermediary need not have knowledge that it has facilitated access.

(c) *Necessity*

The claimant must demonstrate that the injunction is necessary to protect its legitimate interests. Blocking, de-indexing and other invasive orders against intermediaries are digital remedies of last resort — they apply only where all other reasonable means of securing prevention of the wrongful

---

[38] Cf *Redland Bricks Ltd v Morris* [1970] AC 652, 665 (Lord Upjohn) (Lord Reid, Lord Morris, Lord Hodson and Lord Diplock agreeing) ('*Redland Bricks*') (requiring 'a very strong probability on the facts that grave damage will accrue to [the applicant] in the future' if the order is not made).

conduct (such as removal of material or disclosure of the primary wrongdoer) have been exhausted. However, by analogy with *Viagogo*, the applicant should not be required to attempt impracticable methods of removal, such as asking users to install client-side filtering software or bringing proceedings against the primary tortfeasor in an inconvenient forum. Nor would this requirement make relief conditional upon the claimant bringing proceedings against the primary wrongdoer if it would be unreasonable in the circumstances to pursue the primary claim (for example, because of the small scale of the wrong relative to the cost of enforcement, or the low probability of enforcing a judgment).

(d) *Proportionality*

It is now well-established that injunctive relief against an intermediary must be proportionate,[39] in the sense discussed in chapters 5 and 6 for copyright and disclosure remedies. The general approach of English courts is to assess whether the benefits that will be achieved from a measure are proportionate to its costs and other harms[40] — in particular, any interference with other fundamental rights of internet users and intermediaries.[41] In short, the degree of a contested interference must be proportionate to the justification, bearing in mind the 'underlying value' protected by the rights in question.[42] As the CJEU explained in *Promusicae*,[43] this means that 'the measure must be in reasonable proportion to the legitimate aim pursued.'[44] It follows that in any claim for a non-facilitation remedy, the Court faces the difficult task of balancing the proportionality of interfering with intermediaries' rights against the proportionality of restricting those of claimants.[45] This exercise involves the following stages.

(i) *Benefits to the claimant*

The Court's first task is to identify the rights that granting a non-facilitation order would protect. For example, in *Newzbin2*, Arnold J explained that a blocking order was proportionate, given the need to protect the applicants' intellectual property rights, which 'clearly outweigh' the expressive interests of Newzbin2's users and operators, as well as BT.[46] Underlying this assessment of the

---

39 Enforcement Directive arts 3(2), 11(2); Information Society Directive art 8(1); *eBay*, [139]; *Scarlet*, [36].

40 *Redland Bricks*, 666 (Lord Upjohn).

41 See above chapter 5, § 3.3, chapter 6, § 4.3.

42 *Campbell v MGN Ltd* [2004] 2 AC 457, 473–4 (Lord Hoffmann), 489 (Lord Hope) ('*Campbell*').

43 *Promusicae*, [68]–[70]. See also Opinion of the Advocate–General, [54].

44 See also Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk* [2003] ECR I-4989, [83].

45 *Campbell*, 497 (Baroness Hale).

46 *Newzbin2*, [200] (Arnold J).

relative importance of the parties' rights is the (reasonable) assumption that any freedom to express tortious information is relatively weak, since such material by its nature infringes the rights of others and accordingly falls within article 10(2) of the *Convention*. The principal question is how effective the injunction would be in the circumstances.[47]

(ii) *Harms to the respondent and third parties*

The Court must also assess to what extent an injunction would interfere with fundamental rights of ISPs and other third parties. Three considerations are particularly relevant. First, the effect on publishers' article 10 rights is a decisive factor in determining whether restrictions are proportionate.[48] This concern is essentially coterminous with the risk of overblocking: as Arnold J noted in *Newzbin2*, publishers can have only a weak interest in distributing tortious or illegal material, assuming that the rules of primary wrongdoing are themselves compatible with *Convention* and *Charter* rights. Second, the Court should consider the impact on intermediaries — in particular, the feasibility and cost of implementing (and maintaining) an order.[49] The availability of an established blocking or de-indexing system may favour relief.[50] Granularity in time and territory also reduces harm, unlike indefinite or unlimited obligations (as in *Scarlet*).

Third, harms to internet users must be identified; in particular: whether the remedy would entail systematic analysis of their internet browsing; and to what extent their freedom to receive and impart information is restricted. The degree of these interferences will, of course, vary with the scope of the order and the type of restriction sought. Most blocking and de-indexing systems do not analyse or store details of users' personal data, instead examining only the *destination* IP address or indexed data in ways that are identity-agnostic. The risk of overblocking and other 'spill-over harms' must be evaluated in individual cases. The more specific the scope of an order, the more likely it is to be proportionate. In *Newzbin2*, Arnold J held that a domain-wide blocking injunction was appropriate because the website consisted almost exclusively of infringing material, which would make it impracticable for the claimants to produce lists of URLs. However, Arnold J left it as an open question whether this would be an appropriate approach where a website included 'a substantial proportion of non-infringing content'.[51] In general, two-stage filtering at

---

47 See below § 2.4.

48 See, eg, *Giggs (previously known as CTB) v News Group Newspapers Ltd* [2012] EWHC 431 (QB), [78], [85] (Tugendhat J).

49 See *Newzbin2*, [32], [200] (Arnold J); see above chapter 6, nn 203–205 and accompanying text.

50 As noted above, most English ISPs have implemented advanced systems of blocking for the purpose of filtering child abuse materials.

51 *Newzbin2*, [201].

the level of individual URLs remains the best way to minimise harms to affected website operators and internet users.

(iii) *Pressing social need*

Third, to the extent that interferences relate to freedom of expression, they must be justified by a pressing social need. Chiefly, this depends on the gravity of the primary wrong.[52] For example, cases where tortious material is unlikely to cause serious harm or has already been removed are unlikely to justify further injunctive relief.

(iv) *Less intrusive alternatives*

Unlike disclosure, non-facilitation is an exceptional remedy and should only be available when two obvious alternatives have been exhausted. First, the applicant should be unable feasibly to identify and pursue the primary wrongdoer, whether because hidden, impecunious, too numerous or beyond jurisdiction. Second, the claimant should have taken reasonable steps to have the tortious material taken down at its source; in general, only once that has failed can blocking or de-indexing be considered the least intrusive way to protect the claimant's rights. They should, in other words, normally be remedies of last resort.[53] The exception is where strictly territorial interests (such as national reputations or trade marks) are being protected, in which case domestic blocking may be a more proportionate remedy than global removal.

In some cases, it has been suggested that search engine de-prioritisation (rather than outright de-indexing) may be sufficient to reduce access to contested material without rendering it completely inaccessible.[54] Under this approach, websites which are frequently alleged to contain tortious material would be penalised so as to remove them from the all-important first page of search results. Because fewer than 5 per cent of users click through to the second page,[55] de-prioritisation would, it is said, substantially reduce the visibility of tortious material without resort to de-indexing. There are three basic problems with this argument. First, when users are actively seeking out specific (perhaps salacious) material and do not find it on the first page, click-through rates are likely to be much higher. Second, the relevance penalty and frequency of tortious activity required to trigger de-prioritisation are far from objective; it is difficult to articulate any principled basis for determining when and *to what extent* deprioritisation should occur. Third, de-

---

[52] *Promusicae*, [118].

[53] See European Commission, *Public Hearing on Directive 2004/48/EC and the Challenges Posed by the Digital Environment* (Brussels, 7 June 2011) 1.

[54] See Peter Bradwell, 'Revealed: Proposed New Powers over Search Results' (26 January 2012) <http://openrightsgroup.org/blog/2012/new-powers-over-search-results-proposed>.

[55] Optify Inc, *The Changing Face of SERPs: Organic Click Through Rate* (2011) 4.

prioritisation is in some ways worse than de-indexing, in that it actively compromises the neutrality and accuracy of search results, rather than affecting their completeness. It is more proportionate to display accurately ranked but incomplete search results (with notice of the missing entries) than to display complete but arbitrarily ordered ones.

Another possibility is to allow the infringement to continue subject to the website operator lodging security (effectively an undertaking to pay damages for loss suffered by the claimant). Such a course is now expressly permitted under *Civil Procedure Rules* r 25.1(p), which implements article 9 of the *Enforcement Directive*.[56] In most cases, it is unlikely that an intermediary will wish to indemnify a claimant for damage arising from a third party's activities. Further, English law already refuses an injunction where damages would be adequate.

(v) *Overall assessment*

The remedy proposed in this section is discretionary. Because equitable principles remain relevant to the grant of statutory injunctions, it is suggested that these factors should also be assessed in cases where non-facilitation orders are sought under enactments. Section 171(3) of the *1988 Act* expressly preserves the Court's power to refuse to enforce copyright (including by injunction) on public interest grounds.[57] Equally, the court appears to retain an inherent jurisdiction to refuse to enforce property rights in cases where to do so 'would offend against the policy of the law'.[58] If an injunction is granted, it is an elementary principle that its terms must be clear[59] and specify exactly what the respondent must or must not do.[60] The Court will frame these terms 'to secure a just and equitable result',[61] but if an injunction is incapable of being formulated with precision, it will not be granted.

As discussed previously,[62] properly-limited injunctive relief of this kind is not precluded by European safe harbours, prohibitions on monitoring or upper limits on intellectual property remedies. However, orders could not be framed in general terms which required monitoring or entailed excessive costs; so an ISP could not be ordered to seek out tortious material and prohibit

---

[56] Enforcement Directive art 9; Intellectual Property Office, *Transposition Note for Implementation in England and Wales of the IP Directive* (2005) 9(iii).

[57] See *Holman v Johnson* (1775) 1 Cowp 341, 343 (Lord Mansfield CJ) ('No court will lend its aid to a man who founds his cause of action upon an immoral or an illegal act').

[58] See *Hyde Park Residence Ltd v Yelland* [2001] Ch 143, 167–8 (Aldous LJ) (Stuart-Smith LJ agreeing), 172 (Mance LJ) (dissenting). See also *Attorney General v Guardian Newspapers Ltd [No 2]* [1990] 1 AC 109, 268–9, 282.

[59] *Staver Co Inc v Digitext Display Ltd* [1985] FSR 512; *Columbia Picture Industries v Robinson* [1987] Ch 38; *Video Arts Ltd v Paget Industries Ltd* [1988] FSR 501; *Khorasandrijan v Bush* [1993] QB 727.

[60] *Redland Bricks*, 666–7 (Lord Upjohn).

[61] *Ocular Sciences*, 394 (Laddie J).

[62] See above chapter 6, § 4.1.

transmission of the claimants' marks or copyright works *per se*, and a search engine could not be ordered to remove any URLs which might from time-to-time refer to the claimant by name. Different considerations might apply to cases in which a public authority seeks the de-indexing of material on grounds of public policy or to enforce the criminal law; however, those cases are beyond the scope of this chapter.

2 Blocking, de-indexing and freezing remedies

This section identifies three potential applications of non-facilitation injunctions: website blocking, URL de-indexing and asset freezing orders. The precise nature of the facilitating conduct is unrestricted, but these examples illustrate the power and flexibility of the proposed remedy in dealing with certain forms of internet wrongdoing.

Outright removal of the kind discussed in chapters 4 and 5 doubtless offers several advantages over these orders. First, removal is universal: once data have been removed, they are (subject to caching or mirroring) inaccessible regardless of which ISP is used. Blocking and de-indexing are specific to the targeted ISP or search engine, meaning that separate blocks must be introduced by each intermediary within each jurisdiction. Second, removal is immediate whereas blocking or de-indexing can take several days to propagate throughout a complex network. Asset freezing is an even more indirect mechanism, which simply reduces the ease with which the financial spoils of wrongdoing may be enjoyed a tortfeasor. Third, removal reduces the risk of future tortious activity since the original material is deleted; with blocking and de-indexing, the material remains and could be disseminated further by others. Asset freezing has no direct technical effect on the material at all. Fourth, subject to the risk of repeat postings, removal is absolute; blocking is imperfect and can be circumvented by various means.

These orders offer some benefits over removal. First, they are local and *in personam* remedies, which can be applied to ISPs within a particular jurisdiction without affecting access in other countries, even if the Court has no personal jurisdiction over the primary wrongdoer. While some scholars argue that this fractures and undermines the global nature of the internet,[63] it also offers a degree of territorial granularity that the unwieldy hammer of removal cannot. Remedies can be tailored to the limits of the protected interest (for example, a domestic reputation or infringement of a territorial trade mark) without affecting access to the material in countries

[63] John Palfrey, 'Local Nets on a Global Network: Filtering and the Internet Governance Problem' (2010) (Harvard Public Law Working Paper No 10-41).

where use is considered legitimate or protected by foreign defences. Second, they are temporary: blocks can easily be lifted, but files can be undeleted only with difficulty. As an interim measure, therefore, blocking, de-indexing and freezing better preserve data which may eventuate not to be tortious. Third, they do not require the cooperation of foreign hosts, who may operate beyond the reach of injunctive relief and have commercial or ideological incentives not to remove material. The following sections introduce each type of order, before evaluating their effectiveness and suggesting appropriate limitations to ensure that they are applied proportionately.

2.1 Blocking injunctions

Website blocking injunctions are most commonly sought against ISPs. Although theoretically available against any service provider, in practice only ISPs have sufficient control over network layer infrastructure to make blocking worthwhile. In addition to the proposed equitable blocking injunctions, two forms of statutory remedy are recognised in the United Kingdom. First, injunctions are available against service providers for third parties' copyright infringement. Second, conditional provision is made for a broader statutory order requiring a service provider to block access to an infringing internet location. Each of these options is considered in turn. This section assumes familiarity with five basic filtering technologies: (1) IP address blocking; (2) DNS blocking; (3) URL filtering; (4) Deep Packet Inspection ('DPI'); and (5) hybrid filtering models.[64]

(a) *Service provider injunctions*

Sections 97A and 191JA of the *1988 Act* create statutory blocking remedies consequent upon a finding that a third party has infringed the claimant's copyright or performers' rights, respectively. This is a final injunction which is, in essence, an order under article 8(3) of the Information Society Directive,[65] which provides:

> Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

To succeed the applicant must satisfy four elements. First, the respondent must be a 'service provider', as defined in chapter 2,[66] which includes all retail ISPs. Second, there must have been

---

[64] See Jaani Riordan, 'Website Blocking Injunctions: A Technical Primer' (Paper presented at the 27th BILETA Conference, Newcastle, 29 March 2012) for technical details.

[65] *Newzbin2 Order*, [35] (Arnold J).

[66] *Copyright Act* s 97A(3). See above chapter 2, § 2.1(a).

an infringement of the relevant right by a third party using the respondent's service. Third, the respondent must have actual knowledge of the use of its service by another person to infringe copyright. While this appears to set a high threshold requiring subjective knowledge of a specific infringer, the statutory language is broad and it has been so interpreted. In assessing whether the required standard of knowledge is met, the Court is obliged to consider all relevant circumstances, including whether the respondent received a notice of infringement containing the relevant particulars.[67]

The word 'intermediaries' is not defined by the Directive, but recital (59) confirms that the provision was intended to grant relief against those 'best placed' to bring infringing activities to an end. The legislative purpose of s 97A is thus essentially the same as article 8(3).[68] Namely, the provision is directed at any party 'who carries a third party's infringement … in a network', even where the intermediary is not liable for doing or authorising the doing of the infringing acts.[69] As the CJEU has confirmed, this does not require the intermediary to exercise actual or legal control over the use of its service; it is sufficient merely to supply the connection or network over which rights are infringed.[70] The scope of s 97A is therefore much broader than doctrines of authorisation and joint tortfeasance under English law.[71]

Six cases have considered the application of s 97A in rapid succession. The first was *Newzbin1*,[72] where the Court rejected the website operator's argument that the absence of a valid notice meant it lacked knowledge of infringement; receipt of a notice in the prescribed form is not a precondition of actual knowledge, but merely one factor to be considered. However, Kitchin J confined the injunction to files which infringed the claimants' film copyrights: to enjoin Newzbin from linking to *any* infringing binary content would be 'very uncertain' and encompass works in respect of which the claimants possessed no rights.[73] The Court nevertheless took an imprecise, pragmatic approach to establishing actual knowledge; the existence of infringements 'at large' appears to have been enough, even without knowledge of specific acts or users. Even these limitations seem to have been abandoned in later cases.

---

67 Ibid s 97A(2).

68 *Newzbin2*, [146] (Arnold J).

69 Information Society Directive arts 5(1)(a), 8(3).

70 *Tele2*, [43]–[46].

71 Further, statutory blocking remedies do not directly recognise the requirement that damages be inadequate. This could mean that an injunction is available even where the website operator specifically contests infringement.

72 See above chapter 5, § 2.1(a).

73 *Newzbin1*, 552 (Kitchin J).

Second, in *Twentieth Century Fox Film Corporation v British Telecommunications plc* a blocking injunction was made against the respondent ISP ('BT') to prevent its services from being used to infringe the applicants' copyrights via the Newzbin website and its phoenix-like successor, Newzbin2.[74] Building on the findings made by Kitchin J in *Newzbin1*, Arnold J held that the Court had jurisdiction to grant the order, because (1) the operators of the website (in combination with BT's subscribers) used BT's services to infringe the applicants' copyrights; and (2) BT had the necessary knowledge. In this regard, knowledge only requires that the service provider actually knew that at least one person was using its service to infringe copyright. Unlike other forms of secondary liability, s 97A does not require knowledge of 'a specific infringement of a specific copyright work by a specific individual.'[75] This is a lower threshold than that which applies to authorisation liability and joint tortfeasorship, but reflects (1) the broader statutory language of s 97A; (2) the necessity of a broad interpretation to make the remedy achieve its stated purpose; and (3) the fact that we are here dealing with injunctive relief rather than the imposition of monetary liability.

This approach is nevertheless a highly permissive interpretation. It is relatively easy for a service provider to discover (or be alerted to) a single infringement carried out using one its IP addresses; the test pays no regard to the volume of infringement or the proportion of non-infringing use. Section 97A does not even require the service provider to know the identity of the person who is engaging in the infringing activity; for all the Court knows, that person could even be a licensee or representative of the applicant (though probably he or she is not). Similarly, the applicant need not establish which copyright work is being infringed and, by extension, need not specifically prove that it has any rights to that work.

Arnold J observed that actual knowledge can be conferred by notice of facts arising from the receipt of a 'sufficiently detailed notice and a reasonable opportunity to investigate the position'.[76] This appears to be so whether or not the ISP did actually investigate the position. In other words, knowledge extends to being put on notice of facts that would suggest to a reasonable person that an infringement of copyright was taking place. This appears to amount to a conclusion that the phrase 'actual knowledge' encompasses constructive knowledge. Of course, given blocking orders may be available under the equitable protective jurisdiction without any knowledge at all, this may be an unimportant distinction. In some respects, *Newzbin2* was a special

---

[74] *Twentieth Century Fox Film Corporation v British Telecommunications plc* [2011] EWHC 1981 (Ch), [11], [204] (Arnold J) ('*Newzbin2*'). The form of order was determined in [2011] EWHC 2714 (Ch), [56] (Arnold J) ('*Newzbin2 Order*').

[75] *Newzbin2*, [148], [157] (Arnold J).

[76] Ibid [149] (Arnold J).

case, since BT accepted that it had actual knowledge of all the facts as found by Kitchin J in *Newzbin1*, which already ruled on the liability of Newzbin and its members in considerable detail. It is therefore conceivable that in future blocking applications the case against the service provider may be weaker.

The terms of the *Newzbin2* injunction required BT to implement CleanFeed, which uses a combination of IP address re-routing and URL blocking.[77] It contemplates the prevention of future infringements of the same kind — though despite the CJEU's comments in *eBay*, it is clear that this prevention extends beyond infringements be committed by the same tortfeasor in respect of the same copyrights.[78] BT was obliged to block access for all downstream subscribers who received CleanFeed-enabled services[79] — in other words, customers could not 'opt out' simply because they do not want filtered access to the internet. By the time the final injunction was granted, Newzbin2's operators had already released proxy circumvention software designed to allow BT's subscribers to continue accessing Newzbin2. In an attempt to defeat the operation of this software and guard against future circumvention, the injunction provided for a mechanism by which additional IP addresses or URLs could be added to the blocking measures. Such locations must have the 'sole or predominant purpose' of enabling or facilitating access to Newzbin2. The applicants bore responsibility for checking the notified data met this condition.[80]

Newzbin2 is the first example of a blocking order being issued against an English ISP. As such, it might be expected that the terms of the order included an allowance for unforeseen technical errors introduced by blocking. For example, BT argued that the injunction should permit it unilaterally to disable CleanFeed blocking if it reasonably considered that network stability or the preservation of other, more important IWF blocking functionality would be compromised. Arnold J refused such an accommodation, largely because problems had not previously been reported with the system.[81] Instead, the order requires BT to obtain the claimants' (or, in urgent cases, the Court's) consent before shutting down the blocking system. This inflexibility is open to the criticism that it compromises network security and stability, and — if adopted as a matter of course — risks limiting the ability of ISPs to make enhancements to

---

77 *Newzbin2 Order*, [6] (Arnold J).

78 Cf *eBay*, [141].

79 *Newzbin2 Order*, [9] (Arnold J).

80 Ibid [12] (Arnold J).

81 Ibid [17] (Arnold J).

their blocking systems and network infrastructure without engaging in a delicate process of negotiation with parties who have limited concern for the interests of ISPs and their customers.

The third[82] and fourth[83] cases to consider s 97A made blocking injunctions against Sky and TalkTalk in almost identical terms. They required each ISP to 'block *or attempt to block* access' to various domain names and IP addresses, along with any others notified by the claimants which had the 'sole or predominant purpose' of enabling or facilitating access to Newzbin2.[84] Both orders were highly specific as to the blocking technology to be employed, which provides certainty about what the ISPs must do to comply and suggests a degree of emerging consensus about blocking best practices. The *Sky* order required URL rerouting rather than blackholing, which redirected all requests for blocked pages to a URL of the claimant's choosing.[85] This improves transparency (since users will be notified of the existence of a block) but gives the claimants complete discretion over the message displayed. Some supervision is desirable to prevent claimants from appropriating any goodwill associated with legitimate activities of the website operator (minor though they may be) and to prevent visitors being misled or coerced into purchasing legitimate content by way of 'settlement'.

Fifth, in *Dramatico* the claimant record companies sought a blocking injunction against six English ISPs to prevent their subscribers from accessing TPB. In a preliminary judgment, Arnold J held that the users and operators of that website infringe copyright, which satisfied the first element of s 97A. In a subsequent decision, Arnold J held that the ISPs had acquired actual knowledge from previous notifications sent to them, as well as the claimants' evidence and the first judgment.[86] Although the Court could not simply 'rubber stamp' the order agreed between the parties, blocking was here proportionate for similar reasons to *Newzbin2*. If anything, Arnold J concluded, the scale and proportion of infringing activity made a stronger case for blocking than *Newzbin2*. Because the defendant did not share an IP address with other websites, it was appropriate to require IP address blocking.[87]

---

[82] *Twentieth Century Fox Film Corporation v British Sky Broadcasting Ltd* (Unreported, 12 December 2011, Vos J) ('*Sky*').

[83] *Twentieth Century Fox Film Corporation v TalkTalk Telecom Group plc* (Unreported, 9 February 2012, Arnold J) ('*TalkTalk*').

[84] *Sky*, [1](iii) (Vos J). The notification mechanism contained a built-in overblocking safeguard: the claimant must certify to Sky that any new IP address it proposes does not also host other unrelated websites.

[85] Ibid [1](ii) (Vos J).

[86] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd [No 2]* [2012] EWHC 1152 (Ch), [7] ('*Dramatico [No 2]*'). See above chapter 5, nn 84–87 and accompanying text for discussion of the first judgment.

[87] Ibid [13] (Arnold J).

Finally, in *EMI Records Ltd v British Sky Broadcasting Ltd* the Court issued injunctions under s 97A against six ISPs to block access to three BitTorrent trackers.[88] The trackers functioned similarly to TPB and were plainly liable as primary and secondary infringers. They used the ISPs' services to infringe in the same way as Newzbin2 and TPB, with some 4.3m instances of infringement attributable to the ISPs' subscribers. Accordingly, Arnold J had no hesitation in making the orders sought.[89]

(b) *Site blocking injunctions*

Section 17 of the *DEA* includes a procedure — reserved until declared by the Secretary of State[90] — by which a party may apply for an injunction against any service provider to prevent its service from being used to gain access to an internet location which:

(i) hosts or is likely to make available a substantial quantity of infringing material; or

(ii) is being used to facilitate access to such a location.[91]

'Service provider' is again given the same definition as under s 97A,[92] which would include ISPs. 'Internet location' is left undefined, and potentially includes anything that is accessible using an internet network, such as a website, URL, TLD, IP address, subnet range or individual file. Precisely what constitutes a 'substantial quantity' remains unclear, but would be the subject of future regulation. Like ss 97A and 191JA, s 17 is limited to the blocking of internet locations which facilitate copyright infringement.

Section 17 goes well beyond the remedies required by European law. It is a 'purely domestic provision' with a broader purpose and effect.[93] It is broader than s 97A in four important respects. First, although a service provider must be given notice of the application for an injunction,[94] it is not required to possess knowledge of the primary infringement. Second, an injunction can be triggered by mere facilitation; no tortious connecting factor is necessary. Third, second-degree locations can be enjoined whose only connection to tortious activity is that they are 'likely to be used to facilitate access' to another location at which infringing material may be found, even if no infringement ever occurs using the respondent's service. Fourth, an order under s 17 is outcome-

---

88 *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch).

89 Ibid [102]–[107] (Arnold J).

90 He or she must be satisfied that infringement is having a 'serious adverse effect' on business or consumers and that the regulations offer a proportionate solution: *DEA* s 17(3).

91 *DEA* sub-ss 17(2), (4).

92 *DEA* s 17(12).

93 *Newzbin2*, [138] (Arnold J).

94 *DEA* s 17(6)(a).

based: it appears to require the service provider in terms 'to prevent its service being used to gain access' to the relevant location.

The obligation can be imposed on any class of internet intermediary. What is required of a lower-layer network intermediary to discharge it may differ from what is required of another, higher-layer party: an ISP, for example, might need to inspect every packet passing through its service and drop requests for the target location, whereas a website operator might need to adopt pre-moderation to prevent hyperlinks being uploaded that reference the target location. This form of strict layer agnosticism appears to compromise the end-to-end nature of the internet by requiring intermediaries at one network layer to interfere with activities taking place at other layers. Although ISPs are not obliged to take any specific preventative steps, the practical effect will be to encourage voluntary blocking of material notified by copyright owners.[95]

On the basis of OFCOM's report,[96] the government has indicated that it will not take further steps to implement the provisions of s 17.[97] This conclusion is to be welcomed, given that its wording fails to take account of the available methods of blocking and their effect upon network infrastructure. However, as an extant legal rule, it continues to assert prescriptive force on ISPs and may one day be activated once blocking technology sufficiently matures. If that occurs, it is to be hoped that these elements are clarified in a more balanced way.

2.2 De-indexing injunctions

Search engines and other gateways are the predominant means by which internet publications are discovered and accessed.[98] The methods by which search results are ranked and sorted can be highly influential in determining the extent of damage caused by any tortious activity. A de-indexing injunction orders such a service to disable access to tortious material at a specified internet location. The source material is not itself removed or blocked — anyone who knows the URL may still access it directly or via another hyperlink. Rather, the indexing service is instructed not to display hyperlinks to it, making it harder to access. Traffic to de-indexed material can be expected to decline — and with it, the damage caused by dissemination — on the

---

95 Cf *Amstrad v BPI*, 213–14 (Slade LJ), 219 (Glidewell LJ) (concluding that no action lay for negligently facilitating a third party's infringement of copyright); *CBS*, 1054–5 (Lord Templeman). See also *Paterson Zochonis Ltd v Marfarken Packaging Ltd* [1983] FSR 273, 296 (Robert Goff LJ).

96 See OFCOM, above n 106 (ch 1).

97 Department for Culture, Media and Sport, *Next Steps for Implementation of the Digital Economy Act* (August 2011) 7.

98 Dutton and Blank, above n 1 (ch 1), 22 (search engines used by 84 per cent of internet users).

reasonable assumption that if users do not already know the relevant URL and cannot locate it by means of a search engine or hyperlink, then they are unlikely to stumble upon it accidentally. In a very real sense, websites that are de-indexed cease to exist, instead becoming submerged beneath the trillion unique URLs which are. In this way, de-indexing offers one solution to the problem of 'permanent disfigurement' created by the persistence of digital content.[99]

Two methods of de-indexing should be distinguished. The first relies on a technical standard known as the Robots Exclusion Protocol. By adding the appropriate commands to a file called `robots.txt`, publishers can instruct automated crawlers to ignore specified portions of their websites.[100] Such de-indexing is automatic and instigated by the website operator; most search engines execute these requests as a matter of custom. The second method involves manual removal of a particular URL from an index, webpage or feed. In effect, claimants are using liability rules as non-technical means of regulating search engine technology where other methods of search engine optimisation ('SEO') have failed. Indeed, defensive SEO is sometimes a viable alternative to litigation against the primary wrongdoer for reputational wrongs.

(a) *Private de-indexing practices*

Indexing services face growing pressure to develop more effective methods of voluntarily de-indexing tortious material. For example, in March 2012 the Joint Committee on Privacy and Injunctions concluded that

> it was possible to develop the technology proactively to monitor websites for such material in order that the material does not appear in the results of searches. We find [Google's] objections in principle to developing such technology totally unconvincing. Google and other search engines should take steps to ensure that their websites are not used as vehicles to breach the law and should actively develop and use such technology.[101]

Most search engines have well-established internal procedures for the removal of links to content prohibited by their policies. These procedures are usually described as 'take-down', even though their object is typically to remove hyperlinks to tortious material rather than deleting the material itself.

Private de-indexing practices operate successfully on a large scale and offer low-cost relief to many victims of wrongdoing. However, they suffer from three major defects. First, they reflect

---

[99] Jeremy Waldron, 'Dignity and Defamation: The Visibility of Hate' (2010) 123 *Harvard Law Review* 1596, 1607.

[100] See Google Inc, 'Controlling Crawling and Indexing' (2012) *Google Developers* <http://developers.google.com/webmasters/control-crawl-index/>.

[101] Joint Committee on Privacy and Injunctions, *Privacy and Injunctions — First Report* (2012) ch 4, [115]. The metaphor of vehicles is unfortunate, since manufacturers of sports cars are hardly liable for purchasers' unlawful speeding.

arbitrary criteria as to the degree of notice and proof required, the type of wrongdoing which can support an application, and the extent of removal. They are oriented towards copyright infringement and fail to respond effectively to many other forms of wrongdoing, especially defamation and contempt of court. Second, applications for removal are assessed by employees in accordance with company policies, rather than by judicial bodies in accordance with law and taking account of human rights. Parties who are adversely affected by capricious or arbitrary — but lawful — decisions by indices possess very limited options for internal or external review of a decision, leading to a perception that intermediary decision-makers operate outside the rule of law. This section does not suggest there is a 'right to be indexed'. Instead, it points out that private indexing policies lack legitimacy because the rules — and decisions under them — are not promulgated by public authorities subject to judicial review.

Third, search engines do not operate always provide procedural fairness. They rarely notify applicants or affected parties of a decision, much less communicate reasons for reaching it. When de-indexing does occur, it is often hidden from internet users.[102] Equally, search engines face recrimination regardless of whether they censor or preserve search results; moreover, without any cost-shifting mechanism, they cannot recover their removal costs, and have little incentive to invest in more comprehensive notification, review and monitoring systems. In short, private de-indexing has the potential to be extremely effective, but suffers from all the same shortcomings as notice-and-takedown, and lacks the public legitimacy and transparency of a judicial remedy. Current practices are explained in further detail below.

(i) *Search engines*

Google has the most developed de-indexing policies of any search engine. Those policies permit de-indexing in six circumstances. First, a website which violates the company's webmaster guidelines may be 'sandboxed', which penalises the website in search results. Although few details of this mechanism are publicly known, it appears that sandboxing is applied *ex officio* to websites that use paid, hidden or reciprocal links to inflate their search ranking artificially. It is designed to preserve the integrity of query results and to deter website operators from adopting predatory or unfair SEO practices.

---

[102] Google improved the transparency of search results, displaying a warning notice which states: 'In response to a legal request submitted to Google, we have removed *n* result(s) from this page. If you wish, you may read more about the request at ChillingEffects.org.' See, eg, Google Inc, 'Max Mosley video — Google Search' (3 June 2012) <http://goo.gl/OJCIx>.

Second, Google may remove defamatory or copyright infringing material from its index upon receipt of a valid notification from a court, the claimant or her authorised representative.[103] The notification must specify the relevant URLs and explain why the content is unlawful under an 'applicable law'. Google will assess the complaint and determine whether de-indexing is justified. In February 2013, it received 18,528,185 requests for removal of URLs for copyright infringement alone, up from 1,431,794 in March 2012. Google complied with 99.97 per cent of these requests.[104] UK government removal requests increased by 98 per cent.[105]

Third, Google may de-index websites that publish limited categories of personal information, such as social security and bank account numbers, signatures, and legal names appearing on an adult website which breaches Google's webmaster quality guidelines.[106] However, Google will not de-index other types of personal information without a court order. Fourth, Google may expedite the automatic removal of a cached webpage which has since been deleted or modified by its operator.[107] A cache removal request will automatically update the copy stored in Google's index, preventing users from accessing the original version. Fifth, Google implements the IWF blacklist to remove links to known child abuse materials.[108] Sixth, a party may submit a court order from any jurisdiction requiring the 'removal' of content. Google will assess the order internally and determine whether it is valid, issued by a competent tribunal, and justifies de-indexing.[109]

Although Google's transparency is laudable, the boundaries of its de-indexing policies appear to be arbitrary — or at least designed to minimise expenses and insulate its keyword advertising programmes — rather than to assist claimants. For trade mark infringement, Google states that it is 'not a mediator' of content disputes, and refuses to de-index any page on trade mark grounds.[110] Instead, it advises claimants to contact the relevant website operator directly. For disclosure of private information, Google advises that the claimant 'should try to fix the

---

[103] Google Inc, 'Report Other Legal Removal Issue' (2012) *Help* <http://support.google.com/bin/request.py?contact_type=lr_legalother&product=websearch>.

[104] Database, Google Inc, 'Web Search Copyright Removal Data' (Copy on file with author, 2 April 2013).

[105] Google Inc, 'Transparency Report — Removal Requests' (1 April 2013) <http://google.com/transparencyreport/removals/copyright/>. Detailed statistics for other grounds are unavailable.

[106] Google Inc, 'Keeping Personal Information out of Google' (2012) *Help* <http://support.google.com/webmasters/bin/answer.py?hl=en&answer=164133>.

[107] Google Inc, 'My Removal Requests' (2012) *Webmaster Tools* <http://google.com/webmasters/tools/removals>.

[108] Daphne Keller (Associate General Counsel, Google Europe), Submission to Joint Committee on Privacy and Injunctions, 16 January 2012 (London).

[109] Interview, Anthony House and Dorothy Chou, Policy Directors, Google Inc, 11 May 2012.

[110] Google Inc, 'Removing Content from Google' (2012) *Help* <http://support.google.com/bin/static.py?hl=en&ts=1114905&page=ts.cs>. Different removal policies apply to AdWords keyword advertisements, which have a distinct take-down regime that is not examined in this research.

problem at the source', but will not de-index the material independently.[111] It is unclear why Google is willing to entertain requests to remove search results which infringe copyright but not those which infringe privacy or trade marks.

Similarly, Google excludes certain search queries from auto-completion. Blacklisted queries relate mostly to adult and violent content, though they also encompass copyright infringement.[112] Such queries are not suggested to users as they type. Although not strictly examples of de-indexing, the auto-completion blacklist renders those queries less likely to occur, and indirectly discourages users from accessing tortious search results. Queries related to private information[113] and defamation[114] are not filtered.

Other search engines, such as Microsoft Bing, entertain 'content removal requests' that specify a valid reason for removal.[115] The list of valid reasons reads like a page from Borges' *Celestial Emporium of Benevolent Knowledge*,[116] and includes: cached content, abusive or improperly classified adult content, copyright infringement, malicious or spam content, court-ordered removal, and the nebulous category of 'illegal material'. Like Google's policies, the boundaries of de-indexing remain unclear and appear to be determined on an *ad hoc* basis. This undermines transparency, increases the risk of arbitrary or inconsistent decision-making and reduces the legitimacy of all de-indexing decisions.

(ii) *Social networks*

Similar procedures exist for manual removal of hyperlinks from social networks' indices. For example, clause 5.2 of Facebook's *Statement of Rights and Responsibilities* permits the company to 'remove any content or information' posted to Facebook which it believes violates the Statement or the law.[117] Specific notification procedures also exist for de-indexing content which infringes

---

[111] Google Inc, above n 106.

[112] Google Inc, 'Autocomplete' (2012) *Inside Search* <http://support.google.com/websearch/bin/answer.py?hl=en&answer=106230>.

[113] John Plunkett, 'Google Executives Questioned by MPs over Privacy' (*The Guardian*, 30 January 2012) <http://guardian.co.uk/media/2012/jan/30/google-executives-gilled-mps>. For example, if a user typed the words 'Max Mosley' in 2011, the queries 'Max Mosley Nazi' and 'Max Mosley sex video' were automatically suggested. Their results included links to tortious material.

[114] Anna Leach, 'Google Asked to Bin Autocomplete Results for Japanese Man's Name' (26 March 2012) *The Register* <http:// theregister.co.uk/2012/03/26/google_autocomplete_japan/>.

[115] Microsoft Corporation, 'Bing Content Removal' (2012) <http://support.discoverbing.com/eform.aspx?productKey=bingcontentremoval>.

[116] Jorge Luis Borges, 'The Analytical Language of John Wilkins' in Eliot Weinberger (trans), *The Total Library* (1999) 229, 232.

[117] Facebook Inc, 'Terms of Service' (26 April 2011) <http://facebook.com/legal/terms>.

copyright, trade marks, children's rights, false impersonation policies or local privacy laws.[118] In the latter case, Facebook stipulates that it will review a request to determine whether any action is 'required by relevant privacy laws (located outside the United States)'.[119] Successful use of these notification procedures may result in posts linking to external content being removed. Other postings, such as profile pages, groups and events, will be de-indexed from Facebook's internal search facility as a by-product of removal.

De-indexing by Twitter and other services usually requires the claimant to request the relevant intermediary to alter hosted content (such as a 'tweet' or posting) which contains a hyperlink to the material complained of. For example, in May 2012, the Indian Premier League had tweets removed which linked to websites streaming unauthorised live cricket matches.[120] However, a search for 'ipl stream' on Twitter still yields thousands of other tweets referencing sources purporting to offer infringing content.[121] If both the hyperlinking website operator and the source website operator refuse to intervene, there is usually little a claimant can do to prevent such material from being accessed, absent enforceable injunctive relief.

(b) *De-indexing remedies*

Although English courts have not yet granted de-indexing remedies, there is now increasing judicial recognition that the availability of tortious information in front-page search results can be important. For example, in one privacy case, search rankings were a decisive factor in assessing whether private information had become generally accessible,[122] and therefore whether an injunction to prevent further dissemination would be a *brutum fulmen*.[123] It is suggested that de-indexing is a natural extension of the equitable protective jurisdiction, since directing users to material is clear facilitation of the relevant acts of publication or copying. However, de-indexing would only be appropriate where it is proportionate and no viable alternatives exist.

Proportionality would depend on de-indexing being clearly confined to tortious material. Although there is no 'right to be indexed' (just as the right to freedom of expression in a play carries no right to have it broadcast), it is apparent that restrictions on connectivity and search

---

[118] Facebook Inc, 'Reporting a Violation/Infringement of Your Rights' (2012) <http://facebook.com/help/contact/?id=208282075858952>.

[119] Facebook Inc, 'Report an Unauthorized Photo' (2012) *Help* <http://facebook.com/help/contact/?id=346630525351669>.

[120] See Letter from Indian Premier League to Twitter Inc, 'Re: Infringement Notification via Twitter Complaint' (21 May 2012) *Chilling Effects* <http://chillingeffects.org/dmca512c/notice.cgi?NoticeID=374943>.

[121] See Twitter Inc, 'Twitter / Search — ipl stream' (4 June 2012) <http://twitter.com/search/ipl%20stream>.

[122] *WXY v Gewanter* [2012] EWHC 1601 (QB), [28]–[32], [67]–[71] (Slade J).

[123] *Mosley v News Group Newspapers Ltd* [2008] EWHC 687 (QB), [34]–[36] (Eady J).

can approach a point where freedom of expression is engaged in two ways. First, de-indexing of non-tortious material could restrict listeners' rights to access information, similar to state-imposed restrictions on access to libraries or citizen information bureaux. Second, if an injunction denied publishers of non-tortious material access to an audience or customers, this could engage their rights to impart that material, communicate with others and carry on business. The internet is unlike traditional one-to-many 'broadcasting' platforms such as television and newspapers; as a many-to-many platform, it may require two-sided expression rights. As 'one of the essential foundations of a democratic society',[124] exceptions to this freedom must be construed narrowly and be proportionate to a pressing social need. Accordingly, to be justified 'on cogent grounds recognised by law'[125] de-indexing would need to be confined to URLs containing material that is probably tortious.

The practice is more common in American litigation. For example, in *Hermès International Inc v John Doe 1*, the District Court for the Southern District of New York held that 34 websites selling counterfeit versions of the claimant's handbags should be de-indexed by 'any Internet search engines including … Google, Bing, and Yahoo, and any social media websites including … Facebook, Google+, and Twitter', upon receiving actual notice of the Court's order.[126] Cote J held that, as the defendants were obvious infringers, any of their websites that contained the claimant's trade marks should be removed from search results. Although this is a relatively clear case of infringement, the order was overly broad in that it failed to distinguish between infringing and non-infringing uses of the domain names.

In another trade marks case, the District Court for the District of Nevada went even further, granting an interim injunction that the defendants' 228 websites 'immediately be de-indexed and/or removed from any search results pages of all Internet search engines … and all social media websites'.[127] Both cases demonstrate the power of de-indexing remedies; without traffic from the major indices, the defendants' businesses would be unsustainable and the damage caused to the claimants and consumers would be greatly reduced. In this way, a meaningful injunctive remedy was possible despite many of the websites being hosted in offshore safe havens and content being impractical to remove at its source.

---

[124] See *Stoll v Switzerland* [2007] 5 ECHR 101; *Steel v United Kingdom* [2005] 2 ECHR 87.

[125] *Douglas v Hello! Ltd* [2001] 2 WLR 992, [136] (Sedley LJ).

[126] No 12 Civ 1623 (Unreported, SDNY, 30 April 2012) 10 (Cote J).

[127] *Chanel Inc v Does 400–628*, Case No 2:11-cv-01508-KJD-PAL (Unreported, D Nev, Dawson J, 14 November 2011).

2.3 Asset freezing orders

Platforms that distribute substantial quantities of tortious material rely upon advertising revenue and members' donations to make their activities remunerative and meet the associated financial burden of hosting and disseminating the data. Such services rely upon a small group of payment intermediaries to enjoy the proceeds from the high volumes of traffic they attract. Indeed, the vast majority of this revenue is funnelled through just ten advertising networks and a small number of transaction gateways.[128] This suggests that a logical approach to reducing infringement would be to recognise injunctions which prevented those intermediaries from distributing payments to the operators of platforms which engage in tortious conduct.

This would not involve imposing any monetary liability upon payment intermediaries; it would simply be an extension of the existing *Mareva* injunction, again founded on an ancillary jurisdiction to protect a claimant's legal remedies and uphold the administration of justice. Although chiefly relevant to large-scale copyright infringement, such a remedy could also be applied to safe-havens for defamatory or confidential material. Denying these services access to funding offers a cheap and effective, although indirect, way to prevent future infringements. While it would require existing freezing remedies to be expanded, this section suggests that the change is incremental and supported by sound policy arguments. These are developed below.

(a) *Freezing orders against non-tortfeasors*

CPR 25.1(1)(f) permits the Court to make orders restraining a party from dealing with any assets (whether or not situate in England). Their main purpose is to prevent their dissipation by an actual or potential judgment debtor, thereby preserving the claimant's ability to enforce any judgment made in his favour at trial.[129] Like disclosure, they serve to protect the integrity of the Court's processes by ensuring the 'effective enforcement of its orders'.[130] Because the order effectively imposes an oppressive species of security enforced by contempt sanctions, good reasons are needed for making it. To succeed the claimant had to show a real risk of dissipation of the assets.

---

[128] See USC Annenberg Innovation Lab, *Ad Transparency Report* (5 January 2013) 1.

[129] *Camdex International Ltd v Bank of Zambia [No 2]* [1997] 1 WLR 632, 636 (Sir Thomas Bingham MR). See also *JSC BTA Bank v Solodchenko* [2011] 1 WLR 888.

[130] *Parbulk II AS v PT Humpuss Intermoda Transportasi TBK* [2011] 2 CLC 988, [28] (Gloster J) ('*Parbulk II*'). See also *C Inc plc v L* [2001] 2 Lloyd's Rep 459, [44] (Aikens J) ('*C Inc v L*'); *Cardile v LED Builders Pty Ltd* (1999) 198 CLR 380, 399 (Gaudron, McHugh, Gummow and Callinan JJ) ('*Cardile*').

It has long been accepted that freezing injunctions can also be made against persons against whom the claimant has no substantive cause of action. As Hoffmann LJ reasoned in *Mercantile Group (Europe) AG v Aiyela*, it is enough that such orders are 'ancillary' to a cause of action against another, primary wrongdoer.[131] Steyn LJ (agreeing) observed that it 'ought not to perplex anybody' that such orders can be made.[132] Sir Thomas Bingham MR was similarly 'very pleased to reach that conclusion, for if jurisdiction did not exist the armoury of powers available to the court to ensure the effective enforcement of its orders would in my view be seriously deficient.'[133] All that is required is that A (the claimant) has a claim against B (the primary wrongdoer), which if successful would entitle A to recover assets presently held beneficially by C (the third party respondent). Relief against C would therefore be ancillary to the primary claim against B.[134] In particular, it is 'incidental to' and 'dependent upon' A's claim against B, and therefore satisfies the *Channel Tunnel* requirement.[135] A freezing injunction is not made on the basis that the proceeds of wrongdoing are property belonging to A (or over which C is constructive trustee).[136] Nor does it presuppose any wrongdoing by C. It is simply 'the most realistic and practical form of relief' to preserve the claimant's rights to enforce an *in personam* remedy following a finding that the primary wrongdoer has committed a tort.[137]

Freezing injunctions against payment intermediaries would represent a further extension of this principle in two respects. First, since the remedy is directed at disrupting a source of income derived from civil wrongdoing (and indirectly at the prevention of future such wrongdoing), it should not always be necessary to show a risk of dissipation. Instead, A should be able to rely upon the assets being substantially derived from wrongdoing by B against A — though recent authorities suggest a causal link is strictly unnecessary.[138]

Second, it may be far from obvious that a claimant is entitled to recover all, or any particular amount, of money held by a payment intermediary. On current principles, the order could only be made up to the value of A's claim against B: a so-called 'maximum sum' order.[139] If the purpose

---

131 [1994] QB 366, 376 (Hoffmann LJ) (Sir Thomas Bingham MR and Steyn LJ agreeing).

132 Ibid 377 (Steyn LJ).

133 Ibid (Sir Thomas Bingham MR).

134 *TSB Private Bank International SA v Chabra* [1992] 1 WLR 231, 241–2 (Mummery J) ('*Chabra*'); *Cardile*, 402–3.

135 See *C Inc v L*, [50] (Aikens J).

136 The claimant could not, for example, assert a constructive over assets which merely resulted from a *trespass* to his property rights rather than theft of actual property: *Twentieth Century Fox Film Corporation v Harris* [2013] EWHC 159 (Ch), [16]–[19] (Newey J).

137 *Chabra*, 242 (Mummery J).

138 *Parbulk II*, [55]–[56].

139 *Z Ltd*, 576 (Lord Denning), 583 (Eveleigh LJ), 589 (Kerr LJ); *JSC BTA Bank v Ablyazov* [2009] EWHC 3267 (Comm), [28] (Teare J).

of internet freezing orders is expanded beyond preserving an expected judgment to discourage actual and anticipated wrongdoing against third party claimants, then it would follow that this maximum should be lifted to encompass all assets, including future revenue. Ultimately, however, the appropriateness and scope of such an order should be discretionary and take account of all the factors which make it proportionate or otherwise in the circumstances. Relevant factors might include: the ease with which the online assets could be transferred; their connection to wrongdoing; the gravity and scale of wrongdoing; and the primary wrongdoer's reputation, location and previous behaviour.[140]

In support of this extension, the *Mareva* jurisdiction 'an evolving one which has to remain flexible and adaptable to meet new situations as and when they arise.'[141] Section 37(1) is cast in wide terms and can accommodate an extended order.[142] In *Masri v Consolidated Contractors International (UK) Ltd [No 2]*, Lawrence Collins LJJ cited *Chabra* and *Cardile* before concluding that there was no longer any reason why the Court's orders should be confined to existing legal property. The Court was fully prepared to extend the existing remedy of equitable execution of future debts.[143] These and similar developments led the House of Lords in *Fourie v Le Roux* to describe the present landscape of *Mareva* injunctions as 'unrecognisable' compared to the strict jurisdictional rules observed in *Great Northern Railway* and *The Siskina*.[144] Moreover, s 37(1) should be interpreted consistently with article 9(2) of the Enforcement Directive, which provides for asset seizure and freezing where there is any danger of commercial scale infringement going unremedied. Although the Court should rightly be cautious before making extended orders against non-wrongdoers, it should not be forgotten that payment intermediaries indirectly finance and thereby make possible wrongdoing. As the last 20 years of *Mareva* litigation have demonstrated, it is relatively straightforward and cost-effective for payment intermediaries to disable transactions on precisely specified accounts. They are, in this sense, quintessential least cost avoiders.

---

140 *White Book*, [25.1.25.5].

141 *Parbulk II*, [39]; *Chabra*, 241.

142 Cf *South Carolina Insurance Co v Assurantie Maatschappij 'De Zeven Provincien' NV* [1987] AC 24, 40 (Lord Brandon) (noting that 'although the terms of section 37(1) … are very wide, the power conferred by them has been circumscribed by judicial authority dating back many years').

143 [2009] QB 450, 488–9 (Lord Neuberger and Ward LJ agreeing).

144 *Fourie*, 332–3 (Lord Scott).

(b) *Procedural safeguards*

In *Fourie*, Lord Scott cautioned that freezing injunctions are 'a draconian remedy' and carry the potential to cause injustice. Those concerns are multiplied where the order is made against a neutral third party. The remedy is not proprietary and should not be sought for the collateral purpose of getting security for costs. As Lord Bingham explained, their role is protective and supplementary, and their availability should remain 'closely regulated'.[145]

Several safeguards are important to protect intermediaries and primary wrongdoers. First, like other non-facilitation remedies, the claimant must substantiate her primary claim to a high degree. Second, the claimant must identify with precision the assets alleged to belong to the primary wrongdoer, their relationship to the wrongdoing, and the effect which dissipation would have on future wrongdoing. The payment intermediary must have 'as much certainty as possible' about what must be done.[146] Third, although freezing orders do not depend on an existing substantive claim, they are ancillary to such a claim and if the claimant fails to pursue it, the order may lapse or be discontinued.[147] Fourth, the claimant must inform the intermediary against whom the order is made of all the facts which led to the order.[148] If made without notice, all affected parties should have the opportunity to contest the order at a later *inter partes* hearing.

Fifth, and most importantly, the claimant must undertake to pay the intermediary's reasonable costs of identifying and freezing the assets.[149] The need for additional undertakings to third parties likely to sustain damage, such as creditors, must also be considered.[150] Although an undertaking is discretionary, its object should ordinarily be to ensure that an innocent intermediary 'does not suffer in any way by having to assist and support the course of justice prescribed by the injunction'.[151] In *Searose Ltd v Seatrain (UK) Ltd*, for example, Robert Goff J required the claimant to undertake to reimburse any banks with notice of the *Mareva* order their costs of searching for and freezing the relevant accounts:

---

[145] *Fourie*, 334 (Lord Scott), 322–3 (Lord Bingham).

[146] *Z Ltd v A-Z*, 575 (Lord Denning MR); *Searose*, 897 (Robert Goff J).

[147] Ibid 323 (Lord Bingham), [32]–[37] (Lord Scott).

[148] *Flightwise Travel Service Ltd v Gill* [2003] EWHC 3082 (Ch) (Neuberger J).

[149] *Financial Services Authority v Sinaloa Gold plc* [2011] EWCA Civ 1158.

[150] Practice Direction 25A (Interim Injunctions) [5.1A].

[151] *Z Ltd v A-Z*, 575 (Lord Denning MR), 586 (Kerr LJ).

> Banks are not debt-collecting agencies: they are simply, in this context, citizens who are anxious not to contravene an order made by the court, an order which has been obtained on the application of, and for the benefit of, the plaintiff.[152]

Similar comments apply to internet payment intermediaries, which are not responsible for the claimant's vindication any more than offline banks. An undertaking also encourages the claimant to limit the scope of freezing sensibly.[153] Finally, the remaining limitations proposed in chapter 6 should apply *mutatis mutandis*. These safeguards reflect the heightened risk of freezing orders undermining the freedom of third parties to carry on business.

(c) *Policy justifications*

Expanded freezing orders have the potential to be powerful remedies for deterring large-scale internet wrongdoing. First, being personal orders, the Court can act provided it has *in personam* jurisdiction over the payment intermediary.[154] Because the largest intermediaries typically have a local presence, this remains possible even where wrongdoers are located abroad. Second, as in *Viagogo*, such orders impose few negative consequences on non-infringers since they would be limited to payment accounts associated with substantial wrongdoing. Third, major intermediaries favour greater regulation of payments. A recent Google-sponsored report concluded that 'following the money' is the single most effective way to address internet copyright infringement.[155] PayPal recently began actively monitoring its merchants' platforms for infringing and unlawful content.[156]

Fourth, such orders are tailored to disrupt the business models of commercial infringers. Unauthorised sales of copyright works are marginal. Most infringing content is given away freely, in return for website operators enjoying substantial advertising revenue, upon which at least 86 per cent of file-sharing communities rely.[157] Reducing that revenue reduces their commercial incentive to distribute material, especially where there is a non-zero cost of

---

[152] [1981] 1 WLR 894, 896 (Robert Goff J) ('*Searose*'). See also *Prince Abdul Rahman Bin Turki Al Sudairy v Abu-Taha* [1980] 1 WLR 1268, 1273 (Lord Denning MR).

[153] See also *Galaxia Maritime SA v Mineralimportexport* [1982] 1 WLR 539, 543 (Kerr LJ): (enjoining a port authority from exporting assets on a vessel, but requiring the claimant to compensate the authority for its lost income and administrative overheads).

[154] *Fourie*, 333.

[155] Google Inc, 'Follow the Money to Fight Online Piracy' (2 July 2012) *Europe Blog* <http://googlepolicyeurope.blogspot.de/2012/07/follow-money-to-fight-online-piracy.html>.

[156] Cyrus Farivar, 'PayPal Sets Down Stricter Regulations for File-Sharing Sites' (11 July 2012) *Ars Technica* <http://arstechnica.com/business/2012/07/paypal-sets-down-stricter-regulations-for-file-sharing-sites/>.

[157] Detica, *The Six Business Models for Copyright Infringement* (2012) 3–4.

bandwidth, storage and database infrastructure. If enough revenue can be sequestered, it will eventually become financially unattractive to infringe. While non-commercial incentives to disseminate copyright material may remain, there are obvious practical limits to this kind of charitable distribution.

Recent examples support this logic. When Newzbin2 finally shuttered its doors, this was not because it was ordered to by any court, but for lack of funds. As one spokesperson commented: 'Our servers have been unstable and crashing on a regular basis … and we don't have the money to replace them'.[158] Its English user base was decimated by the blocking orders and the company needed funding to continue indexing copyright works. Rights-holders put pressure on its English payment provider, Kthxbai Ltd, which withdrew its services, leaving it with what Newzbin described as 'no realistic means of taking money'. A freezing remedy could potentially achieve this outcome more quickly and efficiently than years of litigation over authorisation liability and blocking injunctions. Following voluntary screening measures adopted by PayPal, one BitTorrent tracker commented, 'Unless we can figure out some realistic and possible way to do site finances completely PayPal free, it seems like the story of TorrentBytes will end very soon after January 2013.'[159] This indicates the potential for asset freezing orders to function as powerful non-facilitation remedies.

2.4 Effectiveness

The most common criticism made of the remedies considered in this section is that they are not fit for purpose.[160] Short of severing a connection at the physical layer, access can never be entirely prevented: the variables are for whom access will be made difficult and how difficult it will be made. Similarly, de-indexing will often fail to prevent tortious content from metastasising through mirror websites, proxy indices, keyword substitution and peer dissemination. Asset freezing offers few guarantees. Each remedy therefore offers limited protection against determined infringers. As OFCOM concluded in relation to blocking:

> Circumvention of a block is technically a relatively trivial matter irrespective of which of the techniques used. Knowledge of how site operators and end users can work around blocks is widely distributed and easily

---

[158] TorrentFreak, 'Newzbin2, the MPAA's Usenet Enemy #1, Calls it Quits' (29 November 2012) <http://torrentfreak.com/newzbin2-the-mpaas-usenet-enemy-1-calls-it-quits-121129/>.

[159] See, eg, TorrentFreak, 'PayPal Demands Invites to Private BitTorrent Trackers' (8 January 2013) <http://torrentfreak.com/paypal-demands-invites-to-private-bittorrent-trackers-130108/>.

[160] See, eg, Evgeny Morozov, *The Net Delusion: How Not to Liberate the World* (2011) 109.

> accessible on the internet. It is not technically challenging and does not require a particularly high level of skill or expertise.[161]

Effectiveness is an important factor when evaluating the proportionality of blocking or de-indexing, since it follows that a measure possessing known cost and adverse consequences will be less proportionate if it ultimately fails to achieve its intended purpose.

Neither remedy is effective to curtail social systems of dissemination, such as forwarded e-mails and word-of-mouth. If a user discovers interesting but tortious material, then it may be spread privately among peer networks, even if the original website is blocked or de-indexed. Some of this secondary material would then be indexed in search engines; removing mirror URLs could quickly become unmanageable and pointless. This emphasises that access restrictions are inherently incomplete, and most useful: (1) to protect material which has not yet been discovered; (2) to limit the speed with which time-sensitive material diffuses; (3) to limit the time for which material is commonly available (on the reasonable assumption that human memories fade quicker than those of search engines); and (4) to increase the difficulty of sharing large binary files, such as copyright-protected films, videos of private conduct, and dossiers of documents. They are less able to prevent the dissemination of textual information, photographs or information whose import can easily be summarised or re-expressed.

Underblocking, consisting of false negatives, will always exist to some degree. However, this section argues that blocking and de-indexing can nevertheless be effective *as legal remedies* in particular cases. Generalisations about the potential for circumvention tell us little about the practical effect of a remedy on the rights of a specific applicant. It only makes sense to consider whether non-facilitation remedies are effective by reference to the policy objectives and protected interests of specific areas of law. Accordingly, effectiveness will be evaluated separately in relation to each kind of wrongdoing.

(a) *Copyright*

The Enforcement Directive obliges member states to provide effective, proportionate and dissuasive remedies to enforce intellectual property rights.[162] Similarly, *TRIPS* requires Members to provide 'prompt and effective' interim relief, orders to desist from and prevent an infringement, and other enforcement procedures 'so as to permit effective action against any act of

---

[161] OFCOM, above n 106 (ch 1), 51.

[162] Enforcement Directive art 3(2).

infringement'.[163] In its *Final Report* on the Enforcement Directive, the European Commission concluded that 'the currently available legislative and non-legislative instruments are not powerful enough to combat online infringements of intellectual property rights effectively.'[164] Although the report did not directly mention blocking or de-indexing, the Commission made two recommendations which support more powerful forms of injunctive relief. First, although the details of how and when an injunction is available are left to member states, national laws should clarify that injunctive relief against an intermediary does not depend on substantive liability for an infringement. Second, it said that intermediaries should be more closely involved in preventing and terminating online infringements.[165]

In determining whether access restrictions are able to prevent infringement, two considerations are relevant. First, as Consumer Focus has argued,[166] there is the technical question of how far access to the targeted resource can be interdicted. Second, wider effects on the growth of legal markets must be considered. As to technical effectiveness, the record is mixed in copyright cases, and it is difficult to isolate the effect of one national blocking order on overall traffic levels. However, the effect can be appreciable. According to Alexa traffic statistics, overall access to Newzbin and Newzbin2 has fallen by 49 per cent since BT implemented blocking, and the website's global traffic rank has fallen by 900 per cent.[167] The local effect is likely to be even more pronounced, as these are global, rather than UK-specific statistics. Where Newzbin was once a predominantly Anglophone service, UK visitors fell to just 8.5 per cent of the website's traffic.[168] Importantly, traffic to other infringement portals does not appear to have materially increased over the same period.[169]

A similar trend can be observed in Denmark, where unique visitors to TPB reportedly declined from 140,000 to under 10,000 per day following implementation of domestic blocking

---

[163] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1867 UNTS 3 (entered into force 1 January 1995), annex 1C (*Agreement on Trade-Related Aspects of Intellectual Property Rights*) ('*TRIPS Agreement*') arts 41(1), 44(1), 50(1).

[164] European Commission, above n 209 (ch 3) 7.

[165] Ibid.

[166] Consumer Focus, *Response to 'Proposal for Code of Practice Addressing Websites that are Substantially Focused on Infringement'* (19 September 2011) 1.

[167] Alexa Internet Inc, 'Statistics Summary for Newzbin.com' (26 March 2012) <http://www.alexa.com/siteinfo/newzbin.com#>.

[168] Ibid.

[169] See, eg, Alexa Internet Inc, 'Statistics Summary for Demonoid.me' (26 March 2012) <http://alexa.com/siteinfo/demonoid.me>; 'Statistics Summary for Torrentreactor.net' (26 March 2012) <http://alexa.com/siteinfo/torrentreactor.net> (showing growth in line with previous trends).

orders.[170] In Finland, `thepiratebay.org` was the 27th most popular website before a blocking order, and now does not appear at all on the list of the top 10 000 websites. However, `thepiratebay.se`, an exact mirror, appears to hold the 51st position, which suggests that most users have located the mirror. In The Netherlands, `thepiratebay.se` remains the 39th most popular website despite partial blocking, while in Sweden (where blocking is very limited) that website ranks 17th.[171] The traffic rank of `kino.to` slid from around 800 to under 100 000 following its blocking and seizure in Austria.[172] It is difficult to draw any firm conclusions from these data: collection methods vary widely, and do not always take account of circumvention using mirror sites and VPNs. These trends may be partly explicable by the fact that where only some ISPs block a popular file-sharing website, only a certain percentage of consumers are motivated to switch ISPs or circumvent the block. Other factors, such as deliberate changes in domain names and the organic growth of alternative piracy services, doubtless also affect access statistics. However, it appears that blocking can sometimes be associated with substantial reductions in website traffic.

As to the second consideration, the positive effects of blocking and de-indexing in catalysing the adoption of legal services should not be under-estimated. This argument can be simply stated. These measures increase the cost of infringement by adding to search costs (finding a mirror or alternative website), configuration costs (for example, having to download and install proxy or anonymisation software) and in some cases service costs (paying for a VPN provider or new ISP). While different consumers will evaluate these added costs with different price sensitivities, it can be expected that overall levels of infringement will fall. Eventually, the cost of infringement will rise to a point where — when the probabilities of enforcement leading to personal liability and future inconvenience are factored in — it becomes more efficient to pay for content from a legitimate source. Thus, as Arnold J reasoned in *Newzbin2*:

> the cost differential between using Newzbin2 and using a lawful service … will narrow still further. This is particularly true for less active users. The smaller the cost differential, the more likely it is that at least some users will be prepared to pay a little extra to obtain material from a legitimate service.[173]

Moreover, even if most users are willing to invest some additional time and effort to evade a website blocking injunction, many will simply not possess the technical skill required to do so on an ongoing basis. Even the simplest circumvention techniques (such as Tor or a web-based proxy)

---

[170] See *Industrie Neederland BREIN v Ziggo BV*, Case No 374634 [2012] HA ZA 10-3184, LJN BV0549 (Unreported, Rechtbank 's-Gravenhage, 11 January 2012) (trans) [4.35].

[171] Alexa Internet Inc, 'Statistics Summary for Thepiratebay.se' (26 March 2012) <http://alexa.com/siteinfo/thepiratebay.se>.

[172] Alexa Internet Inc, 'Statistics Summary for Kino.to' (26 March 2012) <http://alexa.com/siteinfo/kino.to>.

[173] *Newzbin2*, [196] (Arnold J).

still require a degree of knowledge that many casual infringers lack. In any case, it is difficult to predict how many users would actually take steps to circumvent a block, as Parker J noted in *BT*:

> In theory, some may cease or substantially curtail their unlawful activities …; others may simply seek other means to continue their unlawful activities, using whatever technical means are open. The final outcome is uncertain because it is notoriously difficult accurately to predict human behaviour …[174]

One point that these arguments fail to consider is the degree to which website operators could themselves render blocking injunctions ineffective by (1) altering their URL; (2) arming their users with circumvention tools like TPB did; or (3) shifting to protocols which are more difficult to interdict. Notification mechanisms of the kind used in *Newzbin2*, *Sky* and *TalkTalk* can ward off the use of mirrors; they also increase search costs by requiring users to relocate the website. The second method raises many practical difficulties, particularly when the circumvention tools or instructions are distributed by an independent third party who is not otherwise a tortfeasor. While there may be an argument that such a party joins with users and operators of the service in a common design to infringe copyright, this case may be difficult (or at least costly) to substantiate. Ultimately, methods based on user circumvention involve the same assumptions about human behaviour which Parker J declined to validate in *BT*. Finally, while the potential exists for infringement services to migrate to more sophisticated protocols, this does not make remedies against existing services any less effective.[175]

To maximise the effectiveness of blocking remedies, provision should be made for displaying hyperlinks to legitimate sources of material in place of the infringing substitute a user was attempting to access. However, courts should exercise some supervisory role to ensure that content on redirection pages is neither misleading nor aggressive. Non-facilitation remedies should not be treated with a 'set and forget' mentality. The methods used to implement an order must be re-evaluated periodically as circumvention rises and accuracy falls. Even if they were once effective, they will only *remain* so if viable countermeasures are eventually applied. As Clayton points out:

> the effectiveness of any blocking system, and the true cost of ensuring it continues to provide accurate results, cannot be properly assessed until it comes under serious assault.[176]

---

[174] *BT*, [232] (Parker J).

[175] Eg, TPB has announced that it is converting to 'magnet links' instead of `.torrent` files, which makes it possible to trade files without an announcing tracker server. However, this is unlikely to have any effect upon the operators' liability and the availability of injunctive relief. Similar arguments apply to encrypted BitTorrent transfers, which ultimately still require a portal for locating content.

[176] Richard Clayton, 'Failures in a Hybrid Blocking System' (Paper presented at Workshop on Privacy Enhancing Technologies, Dubrovnik, 30 May 2005) 13.

Blocking and de-indexing are thus ongoing processes of maintenance, countermeasures and circumvention whose effectiveness will change over time.

To be effective at combating certain types of infringement, blocking and de-indexing must be rapid, available as interim measures and, in extreme cases, granted on an *ex parte* basis. The most obvious example where effective interim relief is necessary is to prevent the unauthorised streaming of sporting events and other live content such as performances, or access to pre-release films, software and games. If an unauthorised stream is operative, much of the economic damage may be done to the copyright owner within a matter of hours. Given that it can be impossible to remove such materials at their source within this timeframe, blocking may have a role to play in reducing instances of streaming infringement. Existing statutory remedies involve a prolonged two-part trial, which makes them impractical as preventative measures.[177] Substantial improvements to blocking and de-indexing technology are also required before interim orders will become effective; it can currently take hours or even days to be implemented. However, these remedies may be the only effective recourse against wrongdoing of this kind.

Finally, it is important to remember that these are only three remedies in an armoury of many. While none will be completely effective at occluding access alone, each can form a useful and effective component of a wider suite of remedies designed to reduce access to infringing materials. When deployed together, their efficacy may be far greater than the sum of their individual effects. Complementary remedies are vital for effective relief.[178] It is notable that website blocking has arisen almost exclusively in the context of copyright infringement, at the expense of other forms of intellectual property. For example, the sale of counterfeit medicines over the internet poses considerable challenges for trade mark owners, consumers and national enforcement authorities. Unlicensed internet pharmacies are now widespread, many of which sell illegal or untested medicaments. However, the European Commission has indicated that it does not consider website blocking to be 'an appropriate strategy' for counterfeit products.[179]

In the short term, blocking and de-indexing are likely to cause infringers to shift to unblocked platforms, ISPs or circumvention tools. As it becomes more difficult to access unblocked platforms and blocking technologies increase in accuracy and power, we can expect that the cost and difficulty of engaging in infringing file-sharing will increase. Overall, common-sense dictates that casual infringers will eventually shift to cheaper alternatives, such as

---

[177] See also OFCOM, above n 106 (ch 1), 48.

[178] Ibid 49.

[179] Joe McNamee, 'Four Strikes against Web Blocking in Brussels' (2 November 2011) *European Digital Rights* <http://edri.org/edrigram/number9.21/web-blocking--good-news-eu>.

reasonably priced legitimate sources. The remainder — so-called 'hard core infringers' — are likely to concentrate in small communities using darknets, VPNs and anonymising tools. While it is probably impossible to prevent this kind of activity, it is conceivable that the scale of tortious activity will be substantially curtailed.

(b) *Defamatory material*

Blocking and de-indexing of defamatory material is unlikely to be effective in most cases. Principally, this is because it is much easier to mirror and redistribute textual information — which may be encapsulated in an idea, allegation or rumour — than specific binary content. Any order could be trivially circumvented by anyone who had previously accessed the material, simply by copying and pasting that material onto a social network, document repository or comment box on an unblocked webpage, or by summarising its import in any medium.

Second, as *Giggs (previously known as CTB) v News Group Newspapers Ltd* illustrates, the public imagination is disproportionately captured by attempts to restrict access to information, whether tortious or not. The words with which Tugendhat J began his judgment are instructive:

> There can be few people in England and Wales who have not heard of this litigation. The initials CTB have been chanted at football matches when Mr Giggs has been playing for Manchester United.[180]

It is a curious irony of internet remedies that the greater a claimant's attempt to suppress information, the more likely it is to propagate or 'go viral'.[181] The phenomena of internet memes and social networks have only exacerbated this tendency. Indeed, in the interval of time between a remedy being granted and a webpage becoming inaccessible, millions of people might access and distribute its contents. It can therefore be expected that attempts to enjoin access to defamatory material will generally be counter-productive. Although the same logic applies to copyright-infringing materials, the effort and technical resources required to share text-based information are much lower. The situation would be different if, for example, information were distributed in the form of a film or audio file, which might occupy an intermediate position.

Third, non-facilitation remedies would only provide part of the redress that a claimant seeks. Material is still accessible using other ISPs or search engines, or in other jurisdictions, which means that some amount of information leakage back into the forum is inevitable. In cases involving confidential information, this is even more likely to be unacceptable. It is sometimes

---

[180] *Giggs (previously known as CTB) v News Group Newspapers Ltd* [2012] EWHC 431 (QB), [1] (Tugendhat J).

[181] See above chapter 1, § 2.3 for discussion of the 'Streisand effect'.

said that a secret is like an ice cube[182] — inherently perishable and worthless once melted — and partially blocking access to material it is akin to leaving the freezer door open: it is only a matter of time before the remedy is overtaken by outside forces. In such cases, the claimant, like the proverbial ostrich, may be unaware of the extent of leakage until it is too late to reassert confidentiality.

Subject to these qualifications, blocking may be effective in two circumstances: first, where having succeeded at trial the claimant is unable to have material removed from a foreign website; second, where the claimant is only entitled to protect his reputation in a particular territory. Here, there is no reason to suppose that blocking would not at the very least substantially reduce the future damage that would otherwise be suffered by the claimant. Indeed, blocking may even be more effective than in copyright cases since, curiosity aside, third parties may have less intrinsic desire to find material of which they are unaware. However, there are independent reasons why it may be unwise to grant interim or final non-facilitation remedies in defamation cases — not least the potential for abuse, chilling effects on freedom of expression, prior restraints on publication, and the difficulty of identifying related but non-identical publications.

(c) *Civil order and the administration of justice*

Website blocking and de-indexing are sometimes mentioned in the context of maintaining civil order, particularly as means of preventing jurors from accessing prejudicial materials during criminal trials.[183] Although it is unclear exactly how such a scheme would operate, it appears to contemplate a form of virtual sequestration, which would require jurors' ISPs and search engines to block access to a list of prohibited search keywords, webpages and files for the duration of a trial. Whether this could ever be effective would depend on how comprehensive the blocklist is and whether it was possible for intermediaries to block access on a per-user basis. Juror education and proper directions are likely to be more effective and less intrusive than monitoring and blocking domestic connections.

2.5 Limitations upon non-facilitation

The broad argument advanced in this chapter is that, appropriately limited, non-facilitation remedies can be effective and proportionate responses to internet wrongdoing. However, because

---

[182] *Attorney–General v Newspaper Publishing plc* [1988] Ch 333, 358 (Donaldson MR).

[183] Amelia Hill, 'Judges are Resigned to Jurors Researching their Trials Online' (*The Guardian*, 4 October 2010) <http://guardian.co.uk/law/2010/oct/04/judges-resigned-jurors-online-research>.

of the power intermediaries have to make online content disappear, their use of de-indexing and blocking techniques must be carefully scrutinised. The exercise of these powers is intrinsically invisible in that the *absence* of content is very difficult to discern. Recognising this, the Council of Europe has recommended that access restrictions be subject to strict limits and fair processes:

> In many countries, search engine providers de-index or filter specific websites at the request of public authorities or private parties in order to comply with legal obligations or at their own initiative … Any such de-indexing or filtering should be transparent, narrowly tailored and reviewed regularly subject to compliance with due process requirements. … [A]ccess to independent and accountable redress mechanisms should also be respected in this context.[184]

Accordingly, this section proposes several limitations to guard against the risk of abuse. Like the limitations on disclosure considered in chapter 6, they are designed to limit arbitrary or overzealous intrusions by intermediaries acting at the behest of claimants, and to ensure that courts exercise their discretion correctly — principally by encouraging transparency, accuracy, fair compensation and periodic review. These limitations reflect the long-standing requirement that claimants provide cogent evidence of wrongdoing and insure affected parties against the risk that they are wrong.[185]

(a) *Transparency*

Non-facilitation remedies should be granted transparently. Affected third parties should ordinarily be notified and users told when they attempt to access or search for restricted material. There is inherent tension between seeking to suppress access to tortious information and ensuring that the extent of suppression is adequately disclosed. If users are told too precisely what has been de-indexed or blocked, they may be able to find the material by other means, while tortfeasors may circumvent the restrictions by shifting hosts or URLs. If removal is silent, this removes three important sources of accountability. First, website operators may be unaware of the remedy ever having been granted, and unable to protest an unwarranted order until it is too late to avert harm such as lost traffic. Second, users are unable to identify an excessive injunction as the source of errors, which could also occur for any number of technical reasons. Third, deprived of information about filtering practices, consumers are unable to make a rational choice between competing intermediaries based on their policies and attitude towards non-facilitation claims. Transparency

---

[184] Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines (Adopted 4 April 2012) appendix 1, [14]–[15].

[185] *Hubbard v Vosper* [1972] 2 QB 84, 97–8 (Megaw LJ). See Practice Direction 25A (Interim Injunctions), §5.1(1). Zuckerman, above n 251 (ch 6), 340–3. See now *ACTA* art 2.5(5) (requiring undertakings 'sufficient to protect the defendant and to prevent abuse').

allows these mechanisms to function, increasing accountability and reducing the risk of error or abusive practices.

For example, Orange UK recently began filtering access to civil liberties website *La Quadrature du Net* for its pre-paid subscribers. When subscribers attempted to access the website from their mobile phones, they received the message: 'Orange Safeguard has classified this page as only suitable for people over the age of 18.' (The website did not contain any adult material.) One user reported this message to the website, which publicised the issue. Within days, the website was unblocked, though no explanation was ever supplied as to why.[186] While the lack of transparency about how materials were selected for inclusion in the blacklist is concerning, transparency about the occurrence of blocking enabled the false positive to be identified, reported and corrected. Orange's blocking system thus exhibits at least one of the required attributes of transparency.

To this end, non-facilitation remedies should ordinarily require intermediaries to notify the claimant's identity to affected third parties, who can then decide whether to file a counter-notification (offering an undertaking and self-identification in exchange for access being reinstated to the material) or bring proceedings to obtain a declaration that restrictions are unjustified. Effective notice should not be an absolute requirement because, understandably, it will prove impossible to contact many intermediaries (some of whom may deliberately evade such attempts). However, it is normally desirable for the reasons given in chapter 6.[187] It is consistent with the proposition that a non-facilitation order will not ordinarily be proportionate until an applicant has unsuccessfully attempted to have the material complained of removed at its source.

Both tortfeasors and the public should know, in general terms, the reason for removal, the torts allegedly committed by the third party and the date when restrictions were imposed. For example, if an image is de-indexed because it reproduces the claimant's photographic work, a message declaring 'removed for copyright infringement on 1 January 2013' should be displayed in place of the image in search results. For obvious reasons, users should not be informed of the URL for removed content; however, it may be desirable to describe the general nature of the complainant (for example, 'corporation' or 'government agency'). By extension, the intermediary should be transparent about the criteria which are used to determine whether to restrict access. Finally, intermediaries should publish general statistics of the number of removal requests

---

[186] Alessandra Cappuccini and Gemma Craggs, 'Orange UK blocking La Quadrature du Net' (15 February 2012) *Open Rights Group* <http://www.openrightsgroup.org/blog/2012/orange-uk-blocking-la-quadrature-du-net>.

[187] See above chapter 6, § 4.4(a).

received, acted upon and reverted, broken down by region, type of applicant, reason for removal, and time period.[188]

(b) *Accuracy*

Critics of website blocking and de-indexing raise the spectre of overblocking — false positives which deny access to non-tortious content — to argue that its negative effects outweigh any benefits. As Advocate–General Villalón put it in *Scarlet*, systems of content filtering

> inevitably affect lawful exchanges of content [and] therefore have repercussions for [freedom of expression], if only because the unlawful or lawful nature of a given communication, which depends on the scope of the relevant copyright, varies from country to country and is therefore impossible to grasp through technical means.[189]

The risk of overblocking is difficult to assess in the abstract because the extent of false positives depend on at various choices about the technical and procedural design of blocking or de-indexing systems. In their least granular, most opaque forms, they can seriously undermine access to lawful content. However, in a properly designed, regularly maintained, transparent, territorial and responsive system, there is every reason to suppose that the effects of occlusion can be properly limited to tortious materials.

(i) *Choice of filtering technology*

The accuracy of blocking depends mainly on which technology is used. When implemented alone, IP blocking tends to be the least accurate method, with the greatest potential for false positives. However, unless a server hosts exclusively tortious content, IP blocking is rarely implemented in this way. Instead, it is more commonly used to redirect matching traffic to a second-stage filter which uses DNS, URL or DPI-based methods. URL filtering offers the highest granularity — and the lowest risk of false positives — because it allows specific files or webpages to be blocked without affecting other resources on the same website or server. In practice, most English providers use a two-stage blocking method which minimises the risk of overblocking. Similarly, search engine de-indexing is normally URL-based, and therefore sufficiently granular.

Many overblocking arguments fail to consider this point. Instead critics of non-facilitation remedies invoke straw men, such as IP address blocking or algorithm-based systems of content

---

[188] Google and ChillingEffects.org already publish similar statistics, but in less detail: see Google Inc, 'Transparency Report' (31 March 2013) <http://www.google.com/transparencyreport/removals/copyright/>.

[189] *Scarlet*, Advocate–General's Opinion, [86].

classification (which are notoriously unreliable),[190] equating all blocking systems while dealing with only the least accurate case.[191] However, there exists relatively little empirical evidence of overblocking in response to judicial website blocking orders and best-practice filtering systems.[192] Given that CleanFeed has been in operation for almost a decade, this fact is surprising if overblocking concerns are indeed well-founded.

(ii) *Source of filtering criteria*

Despite marked advances in natural language processing, no algorithm presently exists which can reliably separate tortious from non-tortious content or mirrored from unrelated websites. While it may be possible to identify certain subclasses of video and audio content which infringe copyright based on a checksum library,[193] the multitude of file formats, sampling rates, encoding techniques and splitting points makes it virtually impossible to be comprehensive. In other contexts, the dividing line between fair comment and malicious statement, truth and falsehood, or private and public, is difficult enough for judges to discern — let alone a computer algorithm. Accordingly, any application for an injunction which is premised on automated identification of content is likely to fail to some extent. It will either include false positives, leading to overblocking, or it will omit instances of tortious material. For this reason, courts must take care to examine each URL in respect of which relief is sought by a claimant, and not to permit the automatic identification of mirrored content until identification algorithms further evolve.

Most of the handful of temporary and highly publicised false positives relate to deficiencies in the procedures of administrative authorities or private blacklists such as the IWF. These errors led plainly legitimate material to be blocked intentionally, rather than unlisted material to be blocked accidentally. Provided that appropriate procedural safeguards are maintained, decisions by judicial bodies are intrinsically less likely to suffer from these defects. While much could be done to improve the transparency and responsiveness of private blocking mechanisms, suggestions that all forms of blocking *necessarily* produce unacceptable quantities of false positives appear to be exaggerated.

---

[190] See, eg, Daniel Rutter, 'PORNsweeper: Can a Computer Tell a Dirty Picture from a Clean One?' (3 December 2011) *Dan's Data* <http://www.dansdata.com/pornsweeper.htm>.

[191] See, eg, Alexandra Neri, 'Ordering Intermediaries to Implement Filtering Mechanisms: A Controversial Measure with Dreadful Consequences' [2012] 1 *La Semaine Juridique*, 10–11.

[192] See, eg, Open Rights Group, 'Pirate Bay Overblocking — ORG Wiki' (11 May 2012) <http://wiki.openrightsgroup.org/wiki/Pirate_Bay_overblocking> (noting no instances of overblocking caused by the order in *Dramatico*).

[193] See Nathenson, above n 64 (ch 1), 938–44.

(iii) *Territoriality*

Despite moves toward harmonisation of primary copyright norms, there remain significant differences between the scope of protection afforded by national legal systems and secondary liability rules. Those differences are even greater in the case of defamation, which expresses highly localised policy choices about citizens' freedom of expression. In the United States, for example, the First Amendment protects a much wider variety of speech from state regulation than freedoms recognised by English law. As the Advocate–General observed in *Scarlet*, these divergences create the potential for overblocking — but only if blocking is conducted extraterritorially. No issue of disharmonised liability arises if access is denied only by local ISPs in response to domestic requests from persons located within the territory of a member state. For example, suppose website X is hosted abroad in Ruritania, where its content is considered lawful. If an English court orders English ISPs and search engines to block access and de-index X, this would not prevent a person in Ruritania from accessing that material through a Ruritanian ISP or search engine. By contrast, if website X were hosted in England, it is much more probable that X would simply be taken down for all.

Equally, if websites or hosts are ordered to block access to nationals from a particular country,[194] content policies are not being enforced extraterritorially — unless the website responds by simply denying access to all users. In practice, this has not occurred. Copyright blocking orders are implicitly territorial since they require the respondent ISP to prevent infringements of domestic copyrights. However, potential remains for extraterritorial overblocking on routers used in international telecommunications exchanges if national measures are not carefully limited to retail, domestic ISPs.[195] Whether a blocking order could be sought in respect of a foreign right remains an untested question, but it seems likely that the Court would have subject matter jurisdiction over the claim.[196]

De-indexing is usually performed on a territorial basis. Twitter recently switched to a policy of blocking access to content on a per-country basis rather than removing it globally,[197] in an attempt to ensure that material is regulated according to local norms and not by the lowest

---

[194] See, eg, *Yahoo! Inc v La Ligue Contre le Racisme et l'Antisémitisme*, 379 F 3d 1120 (9th Cir, 2004); aff'd *en banc*, 433 F 3d 1199 (9th Cir, 2006); cert denied, 126 S Ct 2332 (2006).

[195] See, eg, Cyrus Farivar, 'Internet Content Blocking Travels Downstream, Affects Unwary Users' (12 July 2012) *Ars Technica* <http://arstechnica.com/tech-policy/2012/07/internet-content-blocking-travels-downstream-affects-unwary-users/>.

[196] See *Lucasfilm Ltd v Ainsworth* [2012] 1 AC 208, 243–4 (Lord Walker and Lord Collins JJSC) (Lord Phillips, Lady Hale and Lord Mance JJSC agreeing).

[197] See Twitter Inc, 'Tweets Still Must Flow' (26 January 2012) *Twitter Blog* <http://blog.twitter.com/2012/01/tweets-still-must-flow.html>.

common denominator of global content standards. Search engines use country-specific query filtering — until recently, omitting state-censored results in China, for example.[198] However, if Google complies with an English court order to de-index content, it will remove the material from its index at `google.co.uk`, but not `google.com`. This is intended to prevent users who access its services outside England from being affected by de-indexing in areas where the Court has no jurisdiction to enjoin indexing. However, it results in under-inclusion, since any knowledgeable English user may conduct their searches through `google.com` once informed that material has been removed.[199] Conversely, if material is removed at source under a notice-and-takedown regime, access is denied to all users wherever they are located. Thus, website blocking actually produces *less* overblocking caused by extraterritorial content laws than notice-and-takedown.

(iv) *Complaint mechanisms*

Finally, accuracy depends on the responsiveness of remedies to reports of incorrectly classified content. Broad standing should be available to review non-facilitation injunctions; any affected internet user should have a sufficient interest to have the injunction limited or set aside. Consistent with the Council of Europe's recommendation to provide 'effective and readily accessible means of recourse' in cases of overblocking,[200] a website operator should be at liberty to contest any private blocking or de-indexing claim before an independent tribunal and, if successful, have their costs paid by the original applicant. Additionally, ISPs, search engines and blacklist operators (such as the IWF) should voluntarily offer a review mechanism by which owners of incorrectly blocked or de-indexed material can appeal their exclusion.[201] Like community moderation systems, harnessing the 'wisdom of crowds' is a viable tool with which overblocking can be rapidly identified and corrected.

In urgent cases, an expedited judicial review process should be available. This review would not proceed on the basis of any *legal* obligation positively to index or provide access to material. Google, like any other private index or ISP, can choose in its discretion what material should be excluded, subject to competition law and its contractual terms with webmasters and users. However, as a matter of policy, it is undesirable for intermediaries to go beyond what is *necessary*

---

[198] Kai Lukoff, 'Google's Share of China's Search Market has Fallen from 30% to 18%' (*Business Insider*, 27 October 2011) <http://articles.businessinsider.com/2011-10-27/tech/30326841_1_baidu-iresearch-sohu>.

[199] This may be avoided with a simple tweak so that IP geo-detection systems are used to determine which local search index is relevant to a query, regardless of whether a 2LD or TLD front-end is used.

[200] Council of Europe, Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters (Adopted on 26 March 2008) pt III(v).

[201] See, eg, `blocked.org.uk`, which allows users to report instances of incorrect web filtering: Open Rights Group, 'Report Blocks' (2011) <http://blocked.org.uk/>.

to cease facilitating wrongdoing — since otherwise the additional access restrictions would be unnecessary and disproportionate to the objective of preventing wrongdoing. Only if the Court or another public authority had made such an order would it be judicially reviewable — a further reason for promoting the use of courts.

(c) *Costs*

Like *Norwich Pharmacal* relief, the costs of defending and implementing blocking, de-indexing and freezing orders should ordinarily be borne by claimants.[202] They will rarely if ever be proportionate if the applicant has not first undertaken to pay those costs. However, English courts taken a different view to courts in other member states, reasoning that ISPs should pay for the implementation costs of blocking and the costs of the application to the extent that they oppose it. In *Newzbin2*, for example, the Court rejected an analogy with *Norwich Pharmacal* orders and held that BT should bear the costs of implementing the order. In effect, because BT's services created the problem, it should pay for the solution:

> BT is a commercial enterprise which makes a profit from the provision of the services which the operators and users of Newzbin2 use to infringe the [applicants'] copyright. *As such, the costs of implementing the order can be regarded as a cost of carrying on that business.*[203]

Arnold J acknowledged that the respondent had committed no legal wrong and was 'innocent' in the sense identified by Aldous LJ in *Totalise*.[204] Despite this, the Court considered it appropriate that BT bear its own costs, while leaving open the possibility that, in other cases, claimants would do so. In *Newzbin2*, the costs were 'modest and proportionate' — around £5000 for the initial block and £100 per subsequent notification — which was not 'excessively costly' in the sense prohibited by article 3 of the Enforcement Directive.[205] The claimants were required to bear the costs of the application up until the point at which BT began vigorously opposing the order.[206] Additionally, they were not required to give any cross-undertaking as to damages — unlike the practice in interim injunctions — because here the injunction was final.[207]

The compliance costs of implementing a blocking or de-indexing order are not likely to be high.[208] However, the costs of contesting the hearing are likely to be far greater, depending on

---

[202] See, eg, European Commission, above n 53, 2.

[203] *Newzbin2* [32] (Arnold J) (emphasis added).

[204] *Totalise*, 1240 (Aldous LJ).

[205] *Scarlet*, [36]; *eBay (CJEU)*, [139].

[206] *Newzbin2 Order*, [53]–[54] (Arnold J).

[207] Ibid [35] (Arnold J).

[208] Interview, Jenni Aldrich, Regional Legal Director, Google Australia Pty Ltd (19 December 2011, Sydney).

complexity, especially in test cases. Even insignificant costs faced by an intermediary add up in aggregate. If respondents are unable to oppose a blocking order they consider wrongly sought without liability to pay the applicant's costs, there is a risk that borderline or unjustified orders will be made unopposed. Particularly in these cases, it is preferable for claims to be determined judicially; this imposes no penalty on the claimant, who must only prove what he is already required to prove. Accordingly, the current approach to costs warrants careful reconsideration, for similar reasons to those identified in chapter 6.[209]

An appropriate costs order also assists in preventing the respondent ISP from being placed at a competitive disadvantage compared to other ISPs not forced to bear the costs of remedial action.[210] For example, if an intermediary opposes an order which has been made in identical terms against an identically-situated intermediary, then there are good reasons to require the unsuccessful respondent to pay costs. This would encourage follow-on compliance without the need for duplicative litigation.

Finally, it should be remembered that a successful claimant will be entitled to recover the cost of non-monetary relief in any subsequent action against the primary tortfeasor. The cost of obtaining a non-facilitation injunction (or disclosure, for that matter) is simply another form of damage which the claimant suffers from the primary wrong. If these costs were recoverable on an indemnity basis, it would not matter that the claimant initially paid the intermediary's costs; instead, losses would be transferred to the wrongdoer whose conduct precipitated the claim. Only in cases where the primary wrongdoer cannot satisfy judgment is the claimant is forced to wear his costs. In practice, this may describe many cases, but for the reasons given it remains inappropriate for intermediaries to be burdened with a costs order for mere facilitation.

Ultimately, the best way to improve treatment of costs is simply to reduce them. First, as these remedies become more commonplace, costs can be expected to fall. Second, specialist tribunals or small-claims tracks could be established. Alternatively, a public authority such as the Information Commissioner could be vested with powers to seek certain remedies to protect the rights of individuals. These options are explored further in chapter 8.

(d) *Time*

Restricting access is not a permanent remedy. It is necessary only until tortious activity ceases or source material is removed by another means. For example, if the claimant obtained a remedy

---

[209] See above chapter 6, § 4.5.

[210] See *Newzbin2*, [188] (Arnold J).

directly against the primary wrongdoer, non-facilitation orders would often become otiose — though relief may become necessary against mirror sites. Although permanent injunctions could occasionally be appropriate, the exceptional nature of occlusion will ordinarily warrant sensible return dates being specified — or pre-agreed lapse conditions — to reconsider whether the restrictions remain accurate and effective. This is particularly true in interim applications, where if the claimant takes insufficient steps to advance his primary claim the injunction should ordinarily be discontinued. Otherwise, the procedure may be abused as a cheap mechanism to secure the removal of unwanted internet postings without subjecting the claims to more than cursory judicial scrutiny.

3 Conclusion

Non-facilitation remedies are not panaceas for internet wrongdoing. Although blocking and de-indexing technologies are steadily improving, they cannot be relied upon to prevent access to tortious materials without error. However, they are far from ineffective. Together they have achieved measurable reductions in traffic to portals for copyright infringement, and there is limited evidence of access to lawful content being affected. Asset freezing orders have proved surprisingly able to reduce incentives to engage in primary wrongdoing on a commercial scale. Although these remedies can be circumvented with sufficient knowledge and effort, they can still be proportionate policy responses to primary wrongdoing in particular cases, particularly when deployed in tandem.

Recent judicial and legislative activity has firmly established the place of blocking injunctions within the repertoire of legal remedies for copyright infringement, while the practices of ISPs, search engines, payment intermediaries and public authorities have contributed to consumer acceptance of blocking, de-indexing and freezing remedies in a range of other areas. This experience suggests that such measures can usefully be extended to other torts under a general principle of non-facilitation. As the government has recognised, each remedy must form part of an integrated strategy to address internet torts in a fair and effective manner.[211] They are incomplete remedies that are naturally complemented by notice-and-takedown, disclosure, and claims against primary wrongdoers.

Although these cases illustrate that non-facilitation orders could operate transparently, in a territorially confined manner and consistently with the technical and architectural foundations

[211] Department for Culture, Media and Sport, above n 97, 7.

of the internet, this chapter has suggested that such remedies warrant caution in at least four areas. First, judicial orders should not require intermediaries to be 'internet police' or arbiters of offensive or borderline material. Intermediaries are not well-equipped to determine whether transmitted content is tortious in a particular jurisdiction, and they should not be encouraged to intervene in transmissions or reorder or filter search results.[212] This is said to encourage a move towards private censorship and restrict quasi-public internet spaces without scrutiny or review.[213] Google cites privacy concerns related to non-facilitation obligations:

> Requiring search engines to screen the content of their web pages would be like asking phone companies to listen in on every call made across their networks for potentially suspicious activity.[214]

Such duties are certainly problematic if intermediaries are required to engage in *ex ante* human monitoring, or to take a position on whether content is or is not tortious. However, it is doubtful whether the same harms arise from algorithmic exclusion of content according to pre-determined rules, or following a reasoned court order. No human agent need monitor or record traffic logs or search histories. Provided that decisions about blocking and de-indexing are made by competent judicial authorities and not private entities, the determination of whether to intervene is conducted according to the rule of law rather than the rule of intermediaries.

Second, although there are good arguments that English courts have inherent jurisdiction to grant non-facilitation remedies, significant uncertainty surrounds their availability outside intellectual property cases. As the Commission concluded, there remain 'uncertainties as to which kind of intermediaries, regardless of their liability, may be subject to a specific measure when contributing to or facilitating an infringement.'[215] The absence of a clear statutory remedy may deter claimants from incurring the expense and publicity of a test case.

Third, making intermediaries bear costs unduly interferes with their freedoms and fails to recognise that innocent conduits are not wrongdoers. Although an intermediary which unreasonably resists an order may cease being a conduit, fairness demands that the claimant pay the costs of access restrictions, subject to an indemnity borne by the primary wrongdoer. Although blocking injunctions may differ from *Norwich Pharmacal* orders in several respects, they still share more in common with other forms of floating injunctive relief than remedies for

---

[212] John Allison et al, Letter to United States Congress, 'Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011"' (5 July 2011) 6.

[213] See, eg, European Commission, above n 53, 1.

[214] Josh Halliday, 'Google Should be Forced to Censor Search Results, Say MPs' (27 March 2012) *The Guardian* <http://guardian.co.uk/technology/2012/mar/27/google-under-fire-from-mps>.

[215] European Commission, *Analysis of the Application of Directive 2004/48/EC in the Member States*, SEC(2010) 1589 final, 14.

wrongdoing. The current approach risks pre-emptive compliance by intermediaries and undermines the E-Commerce Directive safe harbours by making service providers pay sums that can be just as substantial as damages.

Fourth, courts and regulators must accept that these remedies cannot singlehandedly solve the policy concerns associated with different types of internet wrongdoing. Courts should not ignore the wider consequences injunctions may inflict upon intermediaries, users' legitimate communications, competition and innovation. Occlusion compromises the end-to-end nature of the internet by requiring network-layer intermediaries to interfere with application-layer activities. It can restrict freedom of expression by hindering access to and publication of lawful communications. Implementation entails opportunity costs for ISPs and the internet-consuming public. These attributes make it imperative to assess each application carefully by reference to principles of effectiveness, transparency, accuracy, cost, market distortions, architectural neutrality and the rights of third parties. Only by holistic assessment can courts fashion a remedy which is both effective and compatible with the future development of internet technologies. This chapter has suggested a framework within which to conduct that assessment and has generally supported the approach of English courts, subject to several additional limitations designed to prevent injunctions which are costly, unfair, unclear, or of disproportionate scope or duration.[216] Assuming that these principles are respected, there is no reason why non-facilitation remedies cannot tackle other forms of civil wrongdoing online.

In some respects, it is surprising that claimants have waited so long to seek injunctive relief against intermediaries. Like disclosure orders, non-facilitation injunctions do not directly impose monetary liability and therefore do not always require proof of secondary wrongdoing. Such obligations are the natural complements of the safe-harbours which protect intermediaries from monetary liability. They mobilise the facilitator to preserve the integrity of the claimant's primary rights without imposing liability for harms caused by the primary tortfeasor. This makes them attractive options for claimants who wish to prevent overseas tortious materials from being viewed by a local public. Claimants' failure to deploy injunctive remedies to date can partly be explained by the focus on monetary liability, which has distracted from more difficult questions of when and how intermediaries can be ordered to restrict access to materials which cannot practicably be removed at their source. The growth of non-facilitation remedies reflects growing

---

[216] Electronic Frontier Foundation, 'Website Blocking — Off the Table in the UK (For Now)' (5 August 2011) *Deeplinks Blog* <https://eff.org/deeplinks/2011/08/website-blocking-table-uk-least-now>.

recognition that injunctive relief can be at least as effective as other remedies for online wrongdoing.

8
Conclusion

Internet technologies reduce the costs of socially valuable activity, but they also facilitate harmful and tortious conduct.[1] That conduct can be carried out more cheaply, with greater anonymity and with wider consequences than any previous medium of dissemination known to history. However, this is only part of the story. Internet services operated by intermediaries also supply rich marketplaces for culture, ideas and identity; they educate, entertain and challenge, promote healthy polities and encourage economic growth. They can, in short, be forces for democratisation. This is not inevitable. A central theme of this research has been how to craft

[1] Danielle Citron, 'Cyber Civil Rights' (2009) 89 *Boston University Law Review* 61, 62–3.

secondary liability rules which preserve those socially valuable uses of the internet while deterring or compensating detrimental ones. Like other purveyors of technology, intermediaries lead a 'double life',[2] at one moment, harbingers of freedom, generativity and trade; at others, tools of oppression, infringement, censorship and 'enclave extremism'.[3] In a system as complex as the internet, the outcome is usually difficult to predict and harder still to control. This presents an ongoing regulatory challenge which must adapt to new forms of wrongdoing in an environment of rapid social and technological change.

This research has shown that monetary liability rules in copyright and defamation actions offer at best limited and partial solutions to tortious uses of intermediaries' technologies. Non-monetary remedies, such as disclosure and non-facilitation orders, furnish more effective complementary mechanisms for identifying and preventing wrongdoing. Together, these remedies strike a delicate and contested balance between the interests of claimants, intermediaries and internet users. The relationships between them are complex and unsettled. Each remedy explored in this research represents one way among many to regulate internet wrongdoing and uphold territorial rights in national courts. They contain several inherent tensions: between immunising intermediaries and holding them to account; encouraging self-regulation and imposing judicial supervision; upholding claimants' rights and protecting internet users' freedoms; streamlining existing remedies and imposing restrictions that make them proportionate and territorial. There are no simple answers to these intractable problems.

Part 1 of this research commenced by reviewing the recent history and literature of intermediary liability rules. Chapter 1 identified the most common reasons for targeting secondary wrongdoers. It then outlined this research and its methodology. Chapter 2 introduced internet intermediaries as functional entities which supply communications and data services within a layered, modular network architecture. Chapter 3 sought to define the concept of secondary liability as legal responsibility which is derivative from a third party's primary liability. Doctrines of secondary liability rules distribute responsibility among multiple blameworthy parties, allowing violations of rights to be recognised even where a person does not directly engage in the wrongful conduct.[4] Uniting the disparate instances are a normatively significant causal or relational link to wrongdoing and a connecting factor which justifies the imposition of liability, sometimes but not always on grounds of economic efficiency.

---

2 See David Noble, *Forces of Production: A Social History of Industrial Automation* (1984) 325.

3 Cass Sunstein, *Republic.com 2.0* (2007) 78–80.

4 Smith cites the example of Henry II, who in procuring Becket's assassination exclaimed, 'Will no one rid me of this meddlesome priest!': Smith, above n 177 (ch 3), 34, fn 71.

Part 2 of this research examined the monetary liability of intermediaries by reference to two areas of law. Chapter 4 analysed the development of secondary defamation doctrines at common law and argued that they are now being used negatively to shield lower-layer intermediaries from *prima facie* liability where they play no active part in wrongdoing. Recent statutory defences reinforce those policies. Chapter 5 conducted a similar exercise for copyright, arguing that infringement is so widespread that *inter partes* solutions to global problems are unlikely to be effective. While generally supportive of streamlined notification obligations, the benefits of graduated response penalties were unlikely to outweigh their costs. Further substantial changes to monetary liability are properly made by Parliament and not the courts.

Part 3 of this research examined non-monetary liability, identifying a tension between the need for stronger injunctive remedies and, in parallel, stricter limitations and procedural safeguards. Chapter 6 traced the evolution of facilitators' duties to identify wrongdoers. That duty is properly owed by internet intermediaries, though it is not absolute and remains limited by the fundamental rights of others. It proposed several new limitations upon intermediaries' disclosure obligations, while defending disclosure as desirable in appropriate cases. Chapter 7 proposed a new class of non-facilitation injunctions by analogy with the equitable protective jurisdiction. It argued that courts already possess the necessary jurisdiction to make blocking, de-indexing and freezing orders against internet intermediaries where they are necessary and proportionate, provided that all reasonable costs of doing so are paid by the claimant.

This chapter draws together eight of these themes and makes eight recommendations to reform secondary liability rules and procedures in ways that improve their proportionality and compatibility with fundamental rights in claims against internet intermediaries.

1 Themes

Courts have always had an unsettled relationship with new technologies. In a claim for public nuisance arising from damage to horses caused by the noise of passing steam engines, the locomotive was described as 'the great roaring, snorting appalling monster vomiting smoke and fire in all directions'.[5] Had the indictment in *Pease* against the railway operator succeeded, England's 'gift to the world'[6] might never have received local investment. In that case, the

---

[5] *R v Pease* (1832) 4 B & Ad 30; 110 ER 366; cited in Mark Wilde and Charlotte Smith, '*R v Pease* (1832)' in Charles Mitchell and Paul Mitchell (eds), *Landmark Cases in the Law of Tort* (2010) 1, 16.

[6] George Trevelyan, *English Social History* (3rd ed, 1946) 531.

nuisance was not actionable because it was authorised by an Act of Parliament.[7] Depriving the landowner of compensation was undoubtedly unjust, as Lord Denning MR observed over a century later,[8] but considered necessary in order to promote innovation in railways and their useful social functions. Later, as railways reached maturity, statutory authorisation ceased being given expressly and liability attached normally in accordance with *Rylands v Fletcher*: as in *Powell v Fall*,[9] where the locomotive owner was strictly liable for a fire caused by sparks.[10]

The regulatory lifecycle embodied in this gradual introduction and withdrawal of immunity is well-known. Faced with harms brought about by new technology, courts are asked to adapt existing liability rules to encompass the new behaviour. Emergent industries then lobby for protection, leading (in this case) to statutory protection designed to nurture a nascent technology towards maturity. Once the harms and benefits of the technology become more fully quantified and their costs able to be internalised, more nuanced rules are adopted — here a reversion to common law liability. This is, of course, a simplified abstraction of a complex political process, but it has obvious parallels with the development of liability rules in actions involving internet intermediaries: once harried, then protected, and now re-emerging as accepted participants in frameworks for upholding specific public policies.

This comparison has limits: unlike railway operators, intermediaries do not now face strict liability, they were never solely protected by statutory innovations, and those protections have not been entirely withdrawn. However, their obligations to remove, filter, modify and identify content are growing. Litigation against them is increasing. Such parties are sometimes called 'the law's canary'[11] because they test the limits of primary wrongdoing, induce claimants to plead new theories of secondary liability, and warn of problems in policy and procedure. The purpose of this research was to map the boundaries of that liability in two areas of private law and identify emerging problems. This research proposes eight main conclusions.

---

7 The principle of statutory authorisation was developed in subsequent cases, including *Vaughan v The Taff Vale Railway Co* (1860) 5 H & N 679; 157 ER 1351, where the railway company was not liable for a fire set by sparks from a train engine: at 688 (Blackburn J).

8 *Allen v Gulf Oil Refining Ltd* [1980] QB 156, 165–7, 169 (Lord Denning MR).

9 (1880) LR 5 QBD 597, 601 (Bramwell LJ) (Baggallay and Thesiger LJJ agreeing).

10 See also *Hammersmith and City Railway Co v Brand* (1869) LR 4 HL 171, 199 (Blackburn J), 202 (Lord Chelmsford).

11 Folsom, above n 3 (ch 3), 49.

1.1 Taxonomy

First, this research examined the nature of an internet intermediary and suggested that they may be divided into a number of distinct categories according to their functions and network layer of operation. In general, intermediaries act as *conduits* for information, services and transactions between third parties. The nature of their intermediation is *technical* and *electronic*, connecting users of the public internet by supplying infrastructure, connectivity, storage, platforms, applications or other services. Intermediaries are secondary *facilitators* rather than primary *originators* of conduct. Intermediaries *aggregate* data and transactions via a one-to-many relationship with their users; this relationship confers considerable power to regulate such users' rights and interests.

Common-sense dictates that different intermediaries should be treated differently. Although safe harbours are properly defined by reference to categories of activity rather than the fleeting winds of application or protocol, those activities are also capable of obsolescence and stated at such high levels of abstraction that they are vulnerable to uncertainty and divergent interpretations. They overlook the importance of architecture to questions of knowledge, neutrality and control. To overcome these problems, chapter 2 proposed a layered model of physical, network and application-layer intermediaries. This model is just as flexible but is both more comprehensive and precise. It allows the important technical and normative differences between classes of intermediary to be realised without resort to metaphor.[12] As Shimko points out, metaphorical reasoning is often misleading because observation of initial similarities can lead to a presumption of literal identity.[13] One important realisation suggested by the layered taxonomy is that more is required for physical and network-layer intermediaries to lose their neutrality and passivity. This explains and reinforces the approach taken by courts in defamation and copyright claims against secondary parties.

1.2 Incrementalism

Second, while liability rules are challenged by the internet, the case law examined in chapters 3–6 invites the conclusion that existing doctrines and remedies are readily capable of adaptation. In defamation actions, the concept of publication, in combination with doctrines of joint tortfeasorship, is sufficiently flexible to accommodate internet publications by intermediaries.

---

[12] Cf *eBay (CJEU)*, 1013 (Advocate–General Jääskinen) (comparing the challenges of trade mark enforcement to Odysseus's voyage between Scylla and Charybdis).

[13] See Keith Shimko, 'Metaphors and Foreign Policy Decision Making' (1994) 15 *Political Psychology* 655.

New principles have emerged to shield defendants from insubstantial claims and insulate many network-layer intermediaries from *prima facie* liability. Liability for copyright infringement hinges on the unsteady criterion of authorisation; although its scope waxes and wanes with each generation of communications technology, its current breadth appears only to encompass non-conduit intermediaries at the application-layer and above. Monetary liability is being substituted with new notification obligations targeted at network-layer intermediaries.

There is a tendency in internet scholarship to neglect history as a guide to interpreting legal texts or creating future policy. This is unsurprising, given that technological change has been so rapid since the late 1980s that few intermediaries have had 'time to ponder the historical significance of their own activity.'[14] Chapters 3–6 of this research sought to offer a more longitudinal picture of intermediary liability, illustrating the iterative growth of secondary liability doctrines at successive junctions in the history of dissemination and copying technologies. Properly understood, these histories show that intermediaries have always played a substantial part in enforcing and disrupting rights, and that both common law and statutory doctrines gradually developed limits on intermediaries' duties to compensate harms arising from their services and technologies. They draw on a rich body of jurisprudence on tortious and equitable secondary liability in offline disputes. These patterns continue to influence and find expression in modern safe harbours and remedial limits which protect internet intermediaries.

Accordingly, the instinct for general statutory regulation of the internet should be resisted. Statutory and treaty-based processes for enacting both primary and secondary liability rules are not immune from influence and rent-seeking. The common law, conversely, has proven itself uniquely able to adapt existing doctrines and remedies to the challenges presented by internet-based information torts. There is every reason to suppose that courts are capable of continuing incrementally to develop them within the existing framework of adversarial litigation. However, this research has also identified serious disadvantages to determinations of secondary liability in litigation: in particular, it is often slow, uncertain, and relies on *ex post* rule-making which can be less efficient and flexible than specific regulatory measures. However, at least where litigation occurs between two powerful parties — here claimants and intermediaries — the nature of the adversarial process is often less prone to rent-seeking than the alternatives.

Because it is unlikely that new legislation will be enacted which accommodates all interests or speaks with absolute clarity, parties remain dependent on courts to interpret and construe laws

---

[14] Langdon Winner, 'Myth Information: Romantic Politics in the Computer Revolution' in Carl Mitcham (ed), *Philosophy and Technology II: Information Technology and Computers in Theory and Practice* (1986) 269, 272.

in balanced and proportionate ways. This is especially true where legislative processes are imperfect, opaque or influenced by entrenched industries. Accordingly, this research has taken care to point out several areas in which courts are failing to accord proper weight to particular interests in the proportionality analysis. These failures do not warrant statutory reform or wholesale abandonment of existing approaches. Nor do they require us to consign the development of intermediary liability to '[t]hat codeless myriad of precedent' and 'wilderness of single instances'.[15] Instead, courts should continue to develop a meaningful body of principles by which the limits of secondary liability can continue to evolve.

1.3 Accountability

Intermediaries are private, predominantly corporate entities without clear accountability mechanisms. There is a clear tension between immunising them from liability (in order to promote freedom and innovation) and holding them to account for violating the rights of their users and the public. Unrestricted liability remains problematic for the reasons discussed in chapters 1 and 3. Total immunity is equally undesirable, since intermediaries have the capacity to act in ways that undermine public policies: as more than one commentator has asked, *quis custodiet ipsos custodes*?[16] Although most intermediaries are not public authorities, they exercise quasi-public functions in regulating speech, identity, property and reputation. They are the essential platforms through which cultural expression, ideas and personal autonomy are realised online. Many of them organise, rank, and classify information in ways that indirectly influence those freedoms: they supply the 'tools through which the democratic potential of the Internet can be advanced or hindered.'[17] Their actions exert a controlling influence upon the exercise of fundamental rights by billions of individuals.

Much of this influence is positive — protecting users' identities from repressive governments, providing conduits for minority speech, supporting robust debate and the 'marketplace of ideas' — but some of it is deeply concerning.[18] Examples abound of intermediaries voluntarily deploying their powers of content regulation in arbitrary or capricious ways. Facebook banned a satirical cartoon from *The New Yorker* because it depicted 'female nipple

---

15 Alfred Tennyson, *Aylmer's Field* (1793) lns 437–8.

16 See Eoin O'Dell, 'Who Will Google Google?' (27 May 2007) *Cearta* <http://www.cearta.ie/2007/05/who-will-google-google/>. See Juvenal, *Satires*, VI.346–8.

17 Emily Laidlaw, 'Private Power, Public Interest: An Examination of Search Engine Accountability' (2008) 17 *International Journal of Law and Information Technology* 113, 145.

18 See Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (2012) 149–65.

bulges'.[19] Amazon withdrew cloud hosting from WikiLeaks following governmental pressure.[20] Intermediaries' content policies are often pharisaical: tortious speech may on one occasion be defended under stronger safe harbours and speech protections in the United States, while on other occasions non-tortious speech may be removed for reasons of political or commercial convenience. Disclosure raises similar concerns: Yahoo refuses to assist English defamation claimants but has voluntarily capitulated to government requests for information about Chinese pro-democracy activists.[21] These policies are frequently enforced without transparency or review.

The lack of shared decision-making criteria and independent review mechanisms is troubling. Intermediaries have become *de facto* judges of privacy and freedom of expression, often supplanting national courts and regulators. As York concludes, application-layer intermediaries now occupy a 'quasi-public sphere' in which both public and private norms regulate information.[22] This is not a new phenomenon, but merely another example of the privatisation of public spaces and infrastructure, from shopping centres and highways to telecommunications cables. Unlike these other spaces, many repose trust and confidence in internet intermediaries by relying on them to conduct activities in private spaces. Even governments can become powerless in the face of uncooperative intermediaries; witness Google's refusal to bow to White House pressure to remove an inflammatory anti-Muslim video in September 2012.[23] There are no simple answers to these problems, which reflect the intractable difficulty of reconciling incompatible national laws — embodying deep underlying differences in their attitudes towards freedom of expression — and the global scale of intermediaries' businesses, which carries obvious commercial imperatives. In this environment, it is understandable that intermediaries' conduct is governed by 'pragmatic, highly subjective' standards which are developed incrementally and inevitably contested by interest groups.[24] Ongoing disagreement about the appropriateness of these standards, and decisions in individual cases, is unavoidable.

This research has identified several general principles which increase accountability without disproportionately harming innovation or internet freedoms. One form of accountability

---

[19] See Robert Mankoff, 'Nipplegate' (*The New Yorker*, 10 September 2012) <http://newyorker.com/online/blogs/cartoonists/2012/09/nipplegate-why-the-new-yorker-cartoon-department-is-about-to-be-banned-from-facebook.html>.

[20] See above fn 104 (ch 1) and accompanying text.

[21] See Khurram Gore, '*Xiaoning v Yahoo!*: Piercing the Great Firewall, Corporate Responsibility, and the Alien Tort Claims Act' (2008) 27 *Temple Journal of Science, Technology and Environmental Law* 97, 98.

[22] Jillian York, *Policing Content in the Quasi-Public Sphere* (2011) 3.

[23] See David Nakamura, 'White House Asked YouTube to Review Anti-Muslim Film' (*The Washington Post*, 14 September 2012) *Post Politics* <http://www.washingtonpost.com/blogs/post-politics/wp/2012/09/14/white-house-asked-youtube-to-review-anti-muslim-film/>.

[24] York, above n 22, 29.

is supplied by non-monetary orders and regulatory schemes which require intermediaries to assist in enforcing claimants' rights in limited, judicially-mediated circumstances. This research has also argued in favour of territorially granular content policies, transparent reporting of enforcement practices, review mechanisms, and prophylactic measures such as educational schemes and discursive remedies. Further accountability mechanisms may be necessary; this research does not comment on whether these mechanisms should take the form of self-regulatory codes of practice or specific legal duties.[25] Instead, it has sought to demonstrate how intermediary liability rules can be used to increase the enforcement of English legal norms online without disproportionately interfering in the rights of intermediaries and internet users. The focus has therefore been on orders *compelling* intermediaries to exercise their regulatory powers over content and individuals.

There is a certain level of hypocrisy in intermediaries deploying rights-based norms to resist government interference in their policies and practices, while failing to uphold the same rights as against their users. This imbalance in regulation — which affords immunity without responsibility — is in clear need of correction. However, this research concludes that secondary liability rules are insufficient, blunt and often inappropriate instruments of regulation; as is now well recognised, they are slow, costly, and ineffective in a global environment. Non-monetary remedies may supply more meaningful redress in individual cases, but they are not designed to generate *positive* norms capable of general application. They aim only to proscribe certain forms of facilitation of tortious conduct by others.

1.4 Non-monetary remedies

Fourth, this research has suggested that new forms of injunctive relief are needed to uphold the rule of law online. All intermediaries can be ordered to disclose information about wrongdoers in their possession under existing equitable principles. Although flexible and effective, this remedy suffers from several procedural defects which encourage over-compliance and disproportionately harm users' rights to privacy and freedom of expression. Chapter 6 offered several reforms to restore balance and proportionality to the use of disclosure orders against intermediaries. Additionally, website blocking, de-indexing and asset freezing orders are emerging as complementary remedies which have the potential to be applied more widely. Filtering and de-

[25] One possibility, not explored in this research, is to reform the *HRA* so as to treat information society service providers above a certain threshold as 'public authorities' who owe duties to act compatibly with human rights. If public norms are not applied in some form to remedial action by and against intermediaries, there is a significant risk that existing protections for human rights will become devalued in a digital environment which is constituted largely by private entities and communications infrastructure.

indexing technologies are steadily improving, and can be effective and proportionate policy responses to wrongdoing in individual cases. They must, however, be treated with caution. Their potential for misuse is extremely high if appropriate judicial safeguards are not developed.

These non-monetary remedies illustrate that the nature of intermediary liability is shifting from monetary liability rules to softer, more nuanced regulatory obligations. Injunctive remedies provide the flexible lever for which courts have been searching for centuries to regulate secondary wrongdoers. Claimants' preoccupation with damages-based remedies has been a distraction. The proper focus should be on identifying principled limits upon injunctions, resolving vital issues of cost and procedure, and correctly describing their juridical and doctrinal basis. Under European law, these remedies are bounded by the nebulous criterion that they must strike a 'fair balance' between the competing rights. This holistic inquiry is a valuable check on the powers of national courts to interfere in the workings of the internet, but remains highly uncertain. This research has proposed an approach centred upon users' and intermediaries' rights and general principles of proportionality, effectiveness and architectural preservation. Correctly applied, these principles ensure that the global ecology of intermediary liability continues to evolve in ways which preserve and foster the enormous potential of the internet for cultural, scientific and economic growth.

1.5 Rights and realism

Fifth, courts and regulators must have greater regard to extrinsic factors when determining the boundaries of liability. While formalistic analysis of orthodox principles will often produce the correct result, remedies and reasoning would be improved by more direct consideration of innovation, network architecture, and the fundamental rights of internet users and intermediaries. These rights are sometimes labelled 'internet freedoms', which describe a bundle of rights to control private information, freedom of expression, data portability, information self-determination, open and transparent access, and respect for property, reputation and dignity. Having regard to these factors reduces the information asymmetry inherent in developing secondary liability rules without knowing how they will affect the value of internet innovation. Legislators often downplay the benefits of new internet technologies, because (1) it is difficult to value innovation before its benefits have been realised;[26] and (2) incumbent industries are generally able to influence policy-making more effectively than new entrants. Providing greater flexibility

[26] See Kenneth Arrow, 'Economic Welfare and the Allocation of Resources for Invention' in National Bureau of Economic Research (ed), *The Rate and Direction of Inventive Activity: Economic and Social Factors* (1962) 609, 614–18.

to courts reduces the impact of this asymmetry by allowing secondary liability norms to be adjusted at the moment of application.

This breed of 'cyber-realism' is more modest in its aims than previous generations of technology utopians. Digital policies should not be divorced from their real-world counterparts or administered by centralised technologists.[27] Courts and regulators need only to develop a nuanced understanding of how internet tools affect existing behaviours and communities, what intermediaries realistically can do to achieve specific policy aims, and what trade-offs those actions entail. Greater regard should be had for the relationships between internet content or services and individual rights and, in particular, the ways in which intermediaries can reinforce or deny their exercise.[28] This analysis must move beyond the rhetoric of 'internet freedom' and striking a 'fair balance' between fundamental rights, to consider which rights *are* actually entitled to priority and why. These considerations are frequently absent from English and European decisions on intermediary liability.

1.6 Limiting liability

Sixth, the principle that neutral intermediaries should not normally bear monetary liability for third parties' tortious activity is now well established in European and international law.[29] This research identified the emergence of similar principles in defamation and copyright disputes. In defamation, Parliament has sensibly reinforced those limits in the *E-Commerce Regulations* and, once enacted, the Defamation Bill. Copyright, meanwhile, shows a similar structure of flexibility and doctrinal limits, backed by safe harbours and another statutory scheme to deter internet infringement using notification and technical remedies. The proposed technical obligations suffer from serious defects and should be abandoned. However, the notification regime is likely to be proportionate, though its effectiveness remains untested. Periodic monitoring and re-evaluation of this policy is required to ensure that its implementation costs do not outweigh its uncertain benefits.

The age in which intermediaries were given a 'free pass' from content regulation and enforcement duties has long passed, if it ever truly existed. Intermediaries, like claimants and tortfeasors, can act as threatening agents requiring restraint *as well as* vulnerable industries

---

[27] See Morozov, above n 160 (ch 7), 318–19.

[28] Frank Pasquale, 'Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing' in Levmore and Nussbaum (eds), above n 85 (ch 1), 107, 122.

[29] See, eg, United Nations Special Rapporteur on Freedom of Opinion and Expression et al, *Joint Declaration on Freedom of Expression and the Internet* (1 June 2011) art 2(a).

needing protection against an army of claimants and governments. Courts and scholars demonstrate growing awareness of this tension. They correctly recognise that intermediaries wield the dual powers of removal and disclosure, which, if misused, can severely harm internet users and society. This recognition enables non-monetary secondary liability rules to be used to shape an answer to the wider question of how intermediaries can be encouraged to exercise their regulatory powers to contribute to the positive evolution of the web — to foster the 'good parts' and discourage the 'bad parts'[30] — for example, by neutralising harmful code or denying access to clients whose security has been compromised.

1.7 Anonymity

Seventh, this research has highlighted the ambiguous relationship between anonymity and wrongdoing in cyberspace. On the one hand, beneficial anonymity permits authors to avail themselves of freedom of expression while avoiding retaliation or other harms; on the other, harmful anonymity empowers authors to engage in wrongdoing with impunity.[31] Intermediaries play a critical and growing role in regulating online anonymity. Given the importance of the rights at issue, that regulation is properly supervised by the courts according to the principles advanced in chapter 6.

1.8 Territoriality

Eighth, just as the rights protected in actions against intermediaries tend to be territorial, the scope of remedies granted against them is normally national. Application-layer intermediaries are increasingly deploying regional filtering and content policies which enable a high degree of granularity in content blocking; other non-monetary remedies, such as disclosure and sequestration, are by nature territorial in their application to stored data or transactions. Google's policies on de-indexing, keyword advertising and search auto-completion are keyed to national rules; its actions are highly granular as to territory. For example, faced with complaints about the anti-Muslim video, YouTube blocked access in several Middle Eastern and Asian countries, but left open access in the United States.[32] YouTube filters videos in Thailand to comply with

---

[30] (as Zittrain would have us do): see Zittrain, above n 122 (ch 2), 165.

[31] Danielle Citron and Helen Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age' (2011) 91 *Boston University Law Review* 1435, 1482–3.

[32] See John Naughton, 'When the Cybermen Serve as Censors' (*The Observer*, 23 September 2012).

laws governing *lese majeste*.[33] Flickr binds users in several Asian countries to local terms of service which require pre-moderation of content.[34] Twitter recently adopted a policy of filtering objectionable tweets on a national level. Google's Blogger removes content based on ccTLDs rather than globally, using IP geolocation to redirect users to the local 2TLD.[35] eBay enforces different listings rules in America and Europe.

Generally, this form of granularity is desirable because it prevents disproportionate side-effects on speech in territories where there is no legal justification for removal.[36] This avoids the accidental export of lowest-common-denominator freedom of expression by globally removing material illegal in just one territory.[37] However, it also creates pressure to capitulate to national political interests — whether for reasons of convenience or to avoid threatened legislative action — and block access in ways that may not be visible to the most vocal user groups in developed countries. The wider implications of these practices are still emerging.

2 Recommendations

This section briefly suggests eight reforms which, if implemented, would go a long way towards increasing fairness and efficiency in English courts' approach to claims against internet intermediaries.

2.1 Defence of disclosure

First, if the primary wrongdoer is identified, contactable, willing to defend the action and capable of giving a remedy, there is no reason in principle to sue an intermediary for damages, and also no reason to order the intermediary to remove the impugned material, assuming that the primary wrongdoer is solvent and gives an appropriate cross-undertaking in damages. By analogy with defamation, the defence of identification should be extended to all information wrongs, not just defamation. However, the availability of disclosure should be assessed according to traditional *Norwich Pharmacal* principles, which better accommodate the countervailing interests of affected users.

---

[33] See OpenNet Initiative, 'YouTube and the Rise of Geolocational Filtering' (13 March 2008) <http://opennet.net/blog/2008/03/youtube-and-rise-geolocational-filtering>.

[34] Yahoo! Inc, 'What are Content Filters?' (2012) *Flickr FAQ* <http://flickr.com/help/filters/>.

[35] BBC, 'Google Changes Enable "Per Country" Blog Takedowns' (2 February 2012) <http://bbc.co.uk/news/technology-16852920>

[36] See Morozov, above n 160 (ch 7), 215.

[37] Equally, this avoids higher speech protections being exported extraterritorially (as in the case of English content hosted by American intermediaries).

2.2 Defence of exhaustion

Second, exhaustion of claims against the primary wrongdoer should ordinarily be a prerequisite to commencing substantive proceedings against any intermediary. Exhaustion is already a *de facto* requirement for injunctive remedies, since the remedy sought must be 'necessary' in the sense that viable alternatives do not exist. This approach should be extended to monetary claims, where the claimant should be required to certify that the primary wrongdoer is either unidentifiable or unlikely to satisfy judgment.

2.3 Non-facilitation injunctions

Third, as proposed in chapter 7, courts should exercise their powers under CPR 25.1 and s 37(1) of the *Senior Courts Act* to order non-tortfeasor intermediaries to restrict access to tortious material under a standard procedure. This would encompass general blocking, de-indexing and freezing orders for all types of wrongdoing, provided that the intermediary is facilitating wrongdoing and an orders is necessary, proportionate and likely to be effective in the circumstances. The contours of this procedure have already been outlined. All costs of the application and compliance should be paid by the claimant, who should also give a cross-undertaking in damages to be paid if the primary claim fails. Unjustified threats provisions should also be considered.

There is normally no need to join the facilitator as a party to an action against the primary wrongdoer, though full notice should be given. Practice Directions should specify appropriate forms of order and the evidentiary standards claimants must meet. Any interested party should have standing to apply to have the order set aside or varied.

2.4 Notification

Fourth, unless serious prejudice can be shown, claimants and intermediaries should ordinarily take reasonable steps to notify affected parties of any remedial action proposed to be taken against their internet content or services. For this purpose, the WHOIS protocol specification could be amended to require an email address to which such notices can be sent. This should be the primary website operator rather than its host or network operations centre.

It would not be appropriate to expand schemes such as the *DEA* to other wrongs, such as defamation and interferences with privacy. Their harmful consequences are not purely economic;

they tend to be felt immediately and are not susceptible of cumulative recovery in the same way as losses stemming from three instances of copying. Moreover, wrongdoing is, in most cases, more infrequent and often raises more context-sensitive issues, such as determining the meaning and imputations of words or an individual's expectation of privacy. In those cases, the simpler approach may be to disclose and litigate immediately.

2.5 Specialist tribunals

Fifth, a good argument exists that a specialist tribunal should be established — whether as an adjunct to the First-Tier Tribunal, as a referral procedure in the small claims track of the Patents County Court or under a new statutory framework — for hearing low-value claims related to internet content, including news publications. Such an Internet Claims Tribunal would offer cheap, speedy determination of claims, and be empowered to order damages, injunctive relief and costs. Parties could apply for review through the existing tribunal structure to the courts. The Tribunal's primary task would be to regulate and advance disclosure and non-facilitation actions in a forum experienced with internet publications and the competing interests, before making a determination on the lawfulness of content under English law and awarding any appropriate injunctive relief, such as blocking and de-indexing. It could also hear disputes about implementation or widening the scope of orders.

Additionally, a UDRP-style arbitration procedure could be developed and inserted into intermediaries' terms of service. Content disputes would then be governed by standard principles under a uniform procedure, subject to appeals to a competent national court. This would assist in ensuring public accountability and transparency, while absolving intermediaries from the need to make decisions about the legality of material and protecting them from incorrect decisions. All intermediaries who comply with such a 'Uniform Internet Content Dispute Resolution Policy' should be entitled to immunity from monetary liability and have their costs paid by the arbitration body from disputants' fees.

2.6 Harmonisation

Sixth, greater harmonisation of secondary liability rules is desirable within the EU. While substantive copyright norms and safe harbours are now relatively harmonised, secondary liability is not. Defamation laws remain subject to the obvious constraints posed by the Treaties and differing national conceptions of primary rights. If primary liability cannot be harmonised, there

is at least a case for stronger enforcement harmonisation, particularly in relation to notice-and-takedown, disclosure, blocking and de-indexing. As the European Parliament has observed:

> we have not yet achieved a fully functioning digital single market for online and communications services in Europe; … the free movement of digital services and cross-border e-commerce is today severely hindered by fragmented rules at national level[38]

Full harmonisation would require substantial changes to domestic law in light of the differences between English and continental procedural systems. At a minimum, partial harmonisation would require attention in the following areas.

(a) *Notice and takedown*

The E-Commerce Directive contemplates removing or disabling access to content, but does not establish any uniform procedures for voluntary or mandatory action by intermediaries. The Commission recently concluded that common procedures are needed to ensure efficient and proportionate enforcement.[39] Currently, the form, timing and content of notices are matters for national law. This has created divergence in the requirements to fix intermediaries with valid notice. In particular, notices often fail to include all required information in an intelligible format. While commonality is desirable, there are limits to what can be achieved by harmonising notification processes. Each intermediary has different systems and processes for complaint-handling, and it would be unwise and costly to attempt standardisation. More pressingly, the creation of mandatory counter-notification procedures, affected party notices, unjustified threats provisions, and clearer limitations upon 'notice-and-stay-down' orders, would go some way towards restoring a fair balance in the notification procedure.

(b) *Scope of safe harbours*

As discussed in chapters 4 and 5, considerable uncertainty surrounds the application of safe harbours to non-traditional intermediaries such as search engines and social networks, whose activities often span multiple protected and unprotected functions. National courts have taken divergent approaches to classifying these application-layer services. Indeed, even within the United Kingdom, suppliers of hyperlinks are treated inconsistently.[40] Greater clarity is needed

---

[38] European Parliament, above n 69 (ch 2), recital (O).

[39] European Commission, above n 141 (ch 3), 43.

[40] See, eg, *R v Rock & Overton* (Unreported, Gloucester Crown Court, 6 February 2010, HHJ Ticehurst) (holding link website operator immune from copyright infringement); cf *United States v O'Dwyer* (Unreported, Westminster Magistrates' Court, 13 January 2012, Purdy J) (holding link website operator guilty of criminal infringement).

governing the interpretation of these provisions and the concepts of 'neutrality' and 'passivity', which case law of the CJEU has largely failed to clarify.

(c) *Scope of injunctive relief*

The injunctive relief considered in chapters 6 and 7 is far from universally recognised. Although the Information Society Directive and Enforcement Directive specify some minimum and maximum standards, injunctive remedies for wrongdoing outside intellectual property cases remain highly fragmented. In particular, the different preconditions and scope of non-facilitation injunctions make it difficult for intermediaries operating in multiple member states to comply with differently-phrased orders. Their efficacy and cost-effectiveness would be substantially improved if cross-border injunctions were available under common principles to enforce Community rights, such as Community trade marks, or individual rights of privacy which are interfered with by tortious activities in another member state.[41]

2.7 Alternatives

Seventh, although this research has focussed on corrective judicial remedies against intermediaries, alternative regulatory solutions should not be ignored.

(a) *Self-regulation*

In upholding copyrights, lawful sources of music and film content have arguably had a greater positive impact than end-user or intermediary litigation. Services such as Spotify, iTunes and Netflix continue to experience rapid growth as they offer fairly priced access to content with comparable convenience and flexibility to pirated sources. In defamation, voluntary cooperation by website operators, search engines and social networks has substantially reduced the need for litigation against intermediaries and primary authors. VeRO programmes of the kind adopted by eBay have improved trust in online marketplaces and reduced the sale of counterfeit goods. Voluntary filtering by ISPs and non-governmental organisations has proved influential in preventing access to unlawful materials, while self-enforcement of terms of service restrict the availability of many of most harmful sources of internet content. Self-regulation by Google has proved particularly effective, with over 99 per cent of copyright complaints being upheld and

[41] Consider, for example, the publication of photographs of a member of the English royal family in France, which subsequently find their way online.

millions of infringing files de-indexed each week at low cost to claimants. Although no market-based measure is completely effective, they indicate that code and community norms can form useful complements to legal remedies.

(b) *Prophylactic measures against primary wrongdoers*

One virtue of notice-and-notice schemes such as the *DEA* is that they deter primary wrongdoing by educating users about their responsibilities. Effective educational programmes reduce the need for intermediaries to enforce primary norms by decreasing the volume of wrongdoing. Such programmes should be pursued more broadly as a complementary strategy to content removal and intermediary liability.

(c) *Alternative dispute resolution*

Cross-border ADR processes modelled on the UDRP could be explored for contested copyright, defamation and other complaints. The objective would be to obtain cheap and rapid expert determination of whether particular content infringes a stated right under national law, or under pre-agreed principles of content regulation. The extent of the right could be determined, adding legitimacy to intermediaries' decisions to act without judicial mandate, subject to limited appeals to national courts. Claimants would initially bear the cost of the procedure, which intermediaries would incorporate into their terms of service to create an anchor of consent by users of their services. The lack of harmonised primary norms in defamation and privacy actions may make this approach more difficult in cross-border contexts, but it warrants further consideration. Intermediaries have strong incentives to reach agreement on common standards and procedures, especially since most are based in a single jurisdiction which shares many areas of common ground with English speech and privacy values.

2.8 Limitations

Finally, there are practical limits to what intermediary liability rules can accomplish. Although they can generate useful incentives and shift loss in efficient ways, their supporting reasons must be carefully weighed and their wider impacts on technology and society considered. Courts and claimants do not always appreciate in advance where those limits lie. Excessive liability will chill innovation in well-understood ways, and will reduce many benefits of the internet as an engine of freedom, commerce and creativity. Equally, in many cases it is wrong to see liability or technology

as answers to more complex social problems, which neglects the underlying causes of internet wrongdoing in markets, communities and families.

Even where liability rules are the preferred regulatory strategy, national rules can exert limited influence upon a global network. Enforcing private rights in domestic courts will increasingly be hampered by the existence of divergent norms in other jurisdictions. This is particularly evident in the wide chasm separating American and European approaches to defamation and personality rights, and the protection of freedom of expression. American hosts supply a 'safe haven' for content which is, in many European countries, considered tortious or unlawful; indeed, as much as 84 per cent of platforms are now hosted there.[42] In addition to obvious economic consequences for European intermediaries and innovators, this makes it unlikely that removal and access restrictions will ever be completely effective.[43] Websites can shift hosts and jurisdiction at minimal cost; blocks may be circumvented; secrets can be re-tweeted; photographs can be mirrored and rehosted.

As a global communications platform, much of this conduct is beyond the reach of English courts. This does not mean it is worthless to attempt to reduce the harm in England from tortious publications abroad by making necessary and proportionate orders. However, courts should be mindful of the limits of their powers and avoid courting futility when to do so would simply undermine public confidence in the administration of justice. In all cases, the question remains how to balance the likely efficacy of an order against the cost and intrusion it represents to intermediaries and internet users.

In an era of austerity measures and stagnant economies, internet technology offers a clear path towards sustainable growth and global competitiveness.[44] European policy-makers should remember that internet intermediaries are at the centre of this growth: they supply infrastructure, generate demand for labour and investment, contribute to living standards, savings and market efficiency. More generally, their services improve people's lives. Policymakers should therefore foster a legal environment in which internet businesses can flourish without fear of disproportionate liability, in which consumers enjoy the full spectrum of internet freedoms and are protected from intrusions upon their fundamental rights, and in which claimants can access

---

[42] See Pingdom AB, 'Hosting Locations of the World's Top One Million Websites' (7 March 2013) <http://royal.pingdom.com/2013/03/07/hosting-locations-2013/>.

[43] James Banks, 'European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation' (2011) 19 *European Journal of Crime, Criminal Law and Criminal Justice* 1, 12.

[44] McKinsey, above n 16 (ch 1), 42.

effective and proportionate forms of redress. Intermediary liability rules play a vital role in making such an environment habitable for innovators and users.

Bibliography

Books

A P Favre, *De la Sophistication des Substances Médicamenteuses, et des Moyens de la Reconnaître* (1812) 8

Adrian Johns, *Piracy: The Intellectual Property Wars from Gutenberg to Gates* (2009) 7

Adrian Zuckerman, *Zuckerman on Civil Procedure: Principles of Practice* (2nd ed, 2006)

— 236, 248, 250, 287

Annette Kur and Thomas Dreier, *European Intellectual Property Law: Text, Cases & Materials* (2013) 47

Barbara van Shewick, *Internet Architecture and Innovation* (2010) 48, 50, 52

Barry Greene and Philip Smith, *Cisco ISP Essentials* (1st ed, 2002) 55

Beames on Costs (2nd ed, 1840) 241

Bernt Hugenholtz et al, *The Recasting of Copyright & Related Rights for the Knowledge Economy* (2006) 143

Bray on Discovery (1885) 241

Brian Leiter, 'Cleaning Cyber-Cesspools: Google and Free Speech' in Saul Levmore and Martha Nussbaum (eds), *The Offensive Internet: Speech, Privacy, and Reputation* (2010) 155 116, 136

Brian Neill and Richard Rampton (eds), *Duncan & Neill on Defamation* (2nd ed, 1983) 130

Cass Sunstein, 'Believing False Rumors' in Saul Levmore and Martha Nussbaum (eds), *The Offensive Internet: Speech, Privacy, and Reputation* (2010) 91 15

Cass Sunstein, *Republic.com 2.0* (2007) 300

Charles Dickens, *The Life and Adventures of Martin Chuzzlewit* (1844 ed) 8

Charles Hollander, *Documentary Evidence* (10th ed, 2009) 190, 203

Charles Mitchell, 'Assistance' in Peter Birks and Arianna Pretto (eds), *Breach of Trust* (2002) 139 80

Christopher Walton (ed), *Charlesworth & Percy on Negligence* (12th ed, 2010) 33

Claire McIvor, *Third Party Liability in Tort* (2006) 89, 93

Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (2007) 7, 13

David Noble, *Forces of Production: A Social History of Industrial Automation* (1984) 300

David Price and Korieh Duodu, *Defamation Law, Procedure & Practice* (3rd ed, 2004) 101

Debora Spar, *Ruling the Waves: Cycles of Discovery, Chaos and Wealth from the Compass to the Internet* (2001) 6

E J Macgillivray, *The Copyright Act, 1911: Annotated* (1912) 145

Eric Goldman, 'Search Engine Bias and the Demise of Search Engine Utopianism' in Berin Szoka and Adam Marcus (eds), *The Next Digital Decade: Essays on the Future of the Internet* (2010) 461 22

Evgeny Morozov, *The Net Delusion: How Not to Liberate the World* (2011) 279, 309, 311

Felix Oberholzer–Gee and Koleman Strumpf, 'File-Sharing and Copyright' in Josh Lerner and Scott Stern (eds), *Innovation Policy and the Economy* (2010) 182

Frank Pasquale, 'Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing' in Saul Levmore and Martha Nussbaum (eds), *The Offensive Internet: Speech, Privacy, and Reputation* (2010) 107 309

George Trevelyan, *English Social History* (3rd ed, 1946) 301

Glanville Williams, *Joint Torts and Contributory Negligence* (1951) 70, 74, 107

Graham Smith, *Internet Law and Regulation* (4th ed, 2007) 191, 229, 235

Guido Calabresi, *The Costs of Accidents: A Legal & Economic Analysis* (1970) 95

Herbert Hart and Tony Honoré, *Causation in the Law* (2nd ed, 1985) 69, 90

Herbert Rose, *A Handbook of Greek Mythology* (1990) 10

Holdsworth, *A History of English Law* (1926) vol 8 101

Hugh Laddie, Peter Prescott and Mary Vitoria, *The Modern Law of Copyright and Designs* (2nd ed, 1995) 146

Jacques Vandamme (ed), *Services of General Interest in Europe* (2004) 87

James Grimmelmann, 'Some Skepticism about Search Neutrality' in Berin Szoka and Adam Marcus (eds), *The Next Digital Decade: Essays on the Future of the Internet* (2010) 435 22

Jillian York, *Policing Content in the Quasi-Public Sphere* (2011) 306

John Gardner, *Offences and Defences* (2006) 90

John Goldberg and Benjamin Zipursky, 'Rights and Responsibility in the Law of Torts' in Donal Nolan and Andrew Robertson (eds), *Rights and Private Law* (2012) 251 89

John Mackie, *Ethics: Inventing Right and Wrong* (1977) 89

John Mitford, *Mitford's Pleading* (4th ed, 1827) 193

Jonathan Zittrain, *The Future of the Internet — And How to Stop It* (2008) 23, 54, 310

Jorge Luis Borges, 'The Analytical Language of John Wilkins' in Eliot Weinberger (trans), *The Total Library* (1999) 229 271

Jürgen Schwarz, *European Administrative Law* (revised ed, 2006) 177

K J M Smith, *A Modern Treatise on the Law of Criminal Complicity* (1991) 90, 93, 300

Karl Kerényi, *The Heroes of the Greeks* (1978) 10

Kenneth Arrow, 'Economic Welfare and the Allocation of Resources for Invention' in National Bureau of Economic Research (ed), *The Rate and Direction of Inventive Activity: Economic and Social Factors* (1962) 609 308

Kevin Kelly, *What Technology Wants* (2010) 28, 29

Langdon Winner, 'Myth Information: Romantic Politics in the Computer Revolution' in Carl Mitcham (ed), *Philosophy and Technology II: Information Technology and Computers in Theory and Practice* (1986) 269 304

Lawrence Freedman, *Kennedy's Wars: Berlin, Cuba, Laos, and Vietnam* (2002) 164

Lawrence Lessig, *Code and Other Laws of Cyberspace* (2nd ed, 2006) 7, 28, 51

Lawrence Lessig, *Free Culture* (2004) 172

Lawrence Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy* (2008) 172

Lord Hoffmann, 'A Sense of Proportion' in Andenas and Jacobs (eds), *European Community Law in the English Courts* (1998) 149 176

Lord Justice Jackson (ed), *The White Book* (2013 ed) 276

Mark Wilde and Charlotte Smith, '*R v Pease* (1832)' in Charles Mitchell and Paul Mitchell (eds), *Landmark Cases in the Law of Tort* (2010) 1 301

Matthew Collins, *The Law of Defamation and the Internet* (2nd ed, 2005)

— 46, 83, 84, 113, 119, 123, 129

Nicholas Emiliou, *The Principle of Proportionality in European Law: A Comparative Study* (1996) 177

Oliver Wendell Holmes, *The Common Law* (first published 1881, 1963 ed) 69

Oliver Williamson, *The Economic Institutions of Capitalism* (1985) 51

Oxford English Dictionary (2nd ed, 1989) 38

Patrick Atiyah, *Vicarious Liability in the Law of Torts* (1967) 40, 68, 72, 79, 103

Patrick Milmo et al (eds), *Gatley on Libel and Slander* (11th ed, 2010) 83, 84

Paul Mitchell, *The Making of the Modern Law of Defamation* (2005) 106

Peter Birks, 'Civil Wrongs: A New World' in *Butterworths Lectures 1990–1991* (1991) 55 66

Peter Watts (ed), *Bowstead & Reynolds on Agency* (19th ed, 2010) 91, 92

Philip James and David Brown, *General Principles of the Law of Torts* (4th ed, 1978) 90

R P Meagher, J D Heydon and M J Leeming, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (6th ed, 2006) 249

Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (2012) 305

Richard Wright, 'The NESS Account of Natural Causation: A Response to Criticisms' in R Goldberg (ed), *Perspectives on Causation* (2011) 285 149

Robert Ellickson, *Order without Law: How Neighbors Settle Disputes* (1991) 28

Robert Stevens, *Torts and Rights* (2007) 35, 68, 80, 90, 91

Roderick Bagshaw, 'Inducing Breach of Contract' in Jeremy Horder (ed), *Oxford Essays in Jurisprudence* (2000) 131 93

Roger Toulson and Charles Phipps, *Confidentiality* (1st ed, 1996) 80

Ronald Dworkin, 'Foreword' in Ivan Hare and James Weinstein (eds), *Extreme Speech and Democracy* (2009) 5 124

Ronald Mann and Jane Winn, *Electronic Commerce* (2nd ed, 2005) 18

Roscoe Pound and Theodore Plucknett, *Readings on the History and System of the Common Law* (3rd ed, 1927) 101

Sam Ricketson, 'Copyright' in Blackshield, Coper and Williams (eds), *The Oxford Companion to the High Court of Australia* (2001) 152 141

Saul Levmore, 'The Internet's Anonymity Problem' in Saul Levmore and Martha Nussbaum, *The Offensive Internet: Speech, Privacy, and Reputation* (2010) 50 230

T R S Allan, *Constitutional Justice: A Liberal Theory of the Rule of Law* (2001) 181

Tony Honoré, 'Necessary and Sufficient Conditions in Tort Law' in D G Owen (ed), *Philosophical Foundations of Tort Law* (1990) 363 149

Tony Weir, *Economic Torts* (1997) 91

Walter Copinger, *The Law of Copyright* (5th ed, 1915) 145

William Blackstone, *Commentaries on the Laws of England* (9th ed, 1783, reprinted 1978) 6

William Landes and Richard Posner, *The Economic Structure of Intellectual Property Law* (2003) 95

William Patry, *Moral Panics and the Copyright Wars* (2009) 176, 183

Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (2006) 6, 7, 10, 14, 31, 50, 53

Journal articles

Alex Castles, 'The Reception and Status of English Law in Australia' (1963) 2 *Adelaide Law Review* 1 6

Alexandra Neri, 'Ordering Intermediaries to Implement Filtering Mechanisms: A Controversial Measure with Dreadful Consequences' [2012] 1 *La Semaine Juridique* 290

Alfred Yen, '*Sony*, Tort Doctrines, and the Puzzle of Peer-to-Peer' (2004) 55 *Case Western Reserve Law Review* 815 40

Alfred Yen, 'Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace' (2002) 17 *Berkeley Technology Law Journal* 1207 10

Andrew Scott and Alastair Mullis, 'The Swing of the Pendulum: Reputation, Expression and the Recentering of English Libel Law' (2012) 63 *Northern Ireland Legal Quarterly* 27 139

Andrew Scott, 'Reframing Libel: Taking (All) Rights Seriously and Where it Leads' (2012) 63 *Northern Ireland Legal Quarterly* 5 139

Anne Barron, '"Graduated Response" *à l'Anglaise*: Online Copyright Infringement and the *Digital Economy Act 2010*' (2011) 3 *Journal of Media Law* 305 174, 176, 179, 185

Anne Cheung and Rolf Weber, 'Internet Governance and the Responsibility of Internet Service Providers' (2008) 26 *Wisconsin International Law Journal* 403 10

Annemarie Bridy, 'ACTA and the Specter of Graduated Response' (2011) 26 *American University International Law Review* 559 12

Annemarie Bridy, 'Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement' (2010) 89 *Oregon Law Review* 81 179

Annemarie Bridy, 'Why Pirates (Still) Won't Behave' (2009) 40 *Rutgers Law Journal* 565 187

Anthony Ciolli, 'Technology Policy, Internet Privacy, and the Federal Rules of Civil Procedure' (2009) 11 *Yale Journal of Law and Technology* 176 228

Arlie Loughnan and Rita Shackel, 'The Travails of Postgraduate Research in Law' (2009) 19 *Legal Education Review* 99 29

Arvind Narayanan et al, 'On the Feasibility of Internet-Scale Author Identification' [2012] *IEEE Symposium on Security and Privacy* 300 16

Assaf Hamdani, 'Gatekeeper Liability' (2003) 77 *Southern California Law Review* 53 96

Assaf Hamdani, 'Who's Liable for Cyberwrongs?' (2001) 87 *Cornell Law Review* 901 7, 17

Bruce Mann, 'Social Networking Websites — A Concatenation of Impersonation, Denigration, Sexual Aggressive Solicitation, Cyber-Bullying or Happy Slapping Videos' (2008) 17 *International Journal of Law and Information Technology* 252 59

Burton Ong, 'Two Tripartite Economic Torts' (2008) 8 *Journal of Business Law* 723 73

Catherine Stromdale, 'Regulating Online Content: A Global View' (2007) 13 *Computer and Telecommunications Law Review* 173 8

Charles Hollander, '*Norwich Pharmacal* Takes Wings' (2009) 28 *Civil Justice Quarterly* 458 193, 200

Colin Lovell, 'The "Reception" of Defamation by the Common Law' (1962) 15 *Vanderbilt Law Review* 1051 100

Cyrus Chung, 'The *Computer Fraud and Abuse Act*: How Computer Science Can Help with the Problem of Overbreadth' (2010) 24 *Harvard Journal of Law and Technology* 233 53

Daniel Defoe, 'Miscellanea' (3 December 1709) 104 *Review VI* 415 7

Daniel Solove, 'A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere' (2006) 84 *Washington University Law Review* 1195 231

Danielle Citron and Helen Norton, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for our Information Age' (2011) 91 *Boston University Law Review* 1435 310

Danielle Citron, 'Cyber Civil Rights' (2009) 89 *Boston University Law Review* 61 299

David Johnson and David Post, 'Law and Borders — The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367 6

David Reed et al, 'Active Networking and End-to-End Arguments' [1998] *IEEE Network* 69 31

Davor Jančić, 'The European Political Order and Internet Piracy: Accidental or Paradigmatic Constitution-Shaping?' (2010) 6 *European Constitutional Law Review* 430 9

Dennis Lievens, 'eBay's Accessory Liability for Counterfeiting — Why Joint Tort Liability Just Doesn't Cut the Mustard' (2011) 42 *International Review of Intellectual Property and Competition Law* 506 40, 81

Dotan Oliar, 'The Copyright–Innovation Tradeoff: Property Rules, Liability Rules, and Intentional Infliction of Harm' (2012) 64 *Stanford Law Review* 951 96

Doug Lichtman and Eric Posner, 'Holding Internet Service Providers Accountable' (2006) 14 *Supreme Court Economic Review* 221 9, 10, 11, 18, 94, 95, 96

Douglas Lichtman and William Landes, 'Indirect Liability for Copyright Infringement: An Economic Perspective' (2003) 16 *Harvard Journal of Law and Technology* 395 11, 96

Ed Baden-Powell and Luke Anthony, 'Case Comment: Digital Economy — Act 2' (2012) 23 *Entertainment Law Review* 130 170

Edward Lee, 'Rules and Standards for Cyberspace' (2002) 77 *Notre Dame Law Review* 1275 48

Edward Lee, 'Warming up to User-Generated Content' [2008] *University of Illinois Law Review* 1459 13

Eirik Cheverud, '*Cohen v Google, Inc*' (2010) 55 *New York Law School Law Review* 333 — 227, 231, 235

Elizabeth Malloy, 'Bloggership: How Blogs Are Transforming Legal Scholarship: Anonymous Bloggers and Defamation: Balancing Interests on the Internet' (2006) 84 *Washington University Law Review* 1187 228

Emily Laidlaw, 'Private Power, Public Interest: An Examination of Search Engine Accountability' (2008) 17 *International Journal of Law and Information Technology* 113 305

Eva Lomnicka, '"Knowingly Concerned"? Participatory Liability to Regulators' (2000) 21 *Company Lawyer* 120 40

Franceso Rizzuto, 'European Union Telecommunications Law Reform and Combating Online Non-Commercial Infringements of Copyright: Seeing through the Legal Fog' (2011) 17 *Computer and Telecommunications Law Review* 75 12, 28

Frank Easterbrook, 'Cyberspace and the Law of the Horse' [1996] *University of Chicago Legal Forum* 207 6

Gary Becker, 'Crime and Punishment: An Economic Approach' (1968) 76 *Journal of Political Economy* 169 17

Gerard McMeel, 'Philosophical Foundations of the Law of Agency' (2000) 116 *Law Quarterly Review* 387, 389–90 91

Golden Eye 244

Graeme Dinwoodie and Rochelle Dreyfuss, 'TRIPS and the Dynamics of Intellectual Property Lawmaking' (2004) 36 *Case Western Reserve Journal of International Law* 95 28

Graeme Dinwoodie, 'The WIPO Copyright Treaty: A Transition to the Future of International Copyright Lawmaking' (2007) 57 *Case Western Reserve Law Review* 751 97

Greg Lastowka, 'Google's Law' (2007) 73 *Brooklyn Law Review* 1327 11, 13

H L A Hart, 'Definition and Theory in Jurisprudence' (1954) 70 *Law Quarterly Review* 37 40

Harrison Moore, 'Misfeasance and Non-feasance in the Liability of Public Authorities' (1914) 30 *Law Quarterly Review* 276 94

Hazel Carty, 'Joint Tortfeasance and Assistance Liability' (1999) 19 *Legal Studies* 489 73, 79, 92

Hew Dundas, 'Russian Billionaires Revisit *Norwich Pharmacal* Orders' (2011) 77 *Arbitration* 362 238

I Trotter Hardy, 'The Proper Legal Regime for "Cyberspace"' (1994) 55 *University of Pittsburgh Law Review* 993 6

Ian Brown, 'Communications Data Retention in an Evolving Internet' (2011) 19 *International Journal of Law and Information Technology* 95 218

Ira Nathenson, 'Civil Procedures for a World of Shared and User-Generated Content' (2010) 48 *University of Louisville Law Review* 911 11, 182, 290

J C Smith and Peter Burns, '*Donoghue v Stevenson* — The Not So Golden Anniversary' (1983) 46 *Modern Law Review* 147 93

James Banks, 'European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation' (2011) 19 *European Journal of Crime, Criminal Law and Criminal Justice* 1 317

James Edelman, 'When Do Fiduciary Duties Arise?' (2010) 126 *Law Quarterly Review* 302 80

James Grimmelmann, 'Saving Facebook' (2009) 94 *Iowa Law Review* 1137 13

James Tumbridge, 'Defamation — The Dilemma for Bloggers and Their Commenters' [2009] *European Intellectual Property Review* 505 118

Jane Ginsburg and Sam Ricketson, 'Inducers and Authorisers: A Comparison of the US Supreme Court's *Grokster* Decision and the Australian Federal Court's *KaZaA* Ruling' (2006) *Columbia Public Law & Legal Theory Working Papers*, Paper 0698 144

Jane Ginsburg, 'Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace' (1995) 95 *Columbia Law Review* 1466 7

Jane Stapleton, 'Choosing What we Mean by "Causation" in the Law' (2008) 73 *Missouri Law Review* 433 37

Jane Strachan, 'The Internet of Tomorrow: The New–Old Communications Tool of Control' (2004) 26 *European Intellectual Property Review* 123 9

Jennifer Arlen and Reinier Kraakman, 'Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes' (1997) 72 *New York University Law Review* 687 17

Jeremy de Beer and Christopher Clemmer, 'Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries' (2009) 49 *Jurimetrics* 375 9, 13, 31

Jeremy Waldron, 'Dignity and Defamation: The Visibility of Hate' (2010) 123 *Harvard Law Review* 1596 268

Jerome Hall, 'Interrelations of Criminal Law and Torts: I' (1943) 43 *Columbia Law Review* 753 90

Jerome Saltzer et al, 'End-To-End Arguments in System Design' (1984) 2 *ACM Transactions in Computer Systems* 277 51

Jim Harper, 'Against ISP Liability' [2005] *Regulation* 31 33

Joel Smith and Darren Meale, 'Legislative Comment: Internet — *Digital Economy Act 2010*' [2010] *European Intellectual Property Review* 75 168

John Palfrey, 'Four Phases of Internet Regulation' (2010) 77 *Social Research* 981 6

John Tehranian, 'Infringement Nation: Copyright Reform and the Law/Norm Gap' [2007] *Utah Law Review* 537 176

Jonathan Zittrain, 'Internet Points of Control' (2003) 44 *Boston College Law Review* 653 40

Jonathan Zittrain, 'Privacy 2.0' [2008] *The University of Chicago Legal Forum* 65 13

Jonathan Zittrain, 'The Generative Internet' (2006) 119 *Harvard Law Review* 1974 48, 52

Juan Cianciado, 'The Principle of Proportionality: The Challenges of Human Rights' (2010) 3 *Journal of Civil Law Studies* 177 177

Julie Cohen, 'Cyberspace as/and Space' (2007) 107 *Columbia Law Review* 210 6

Keith Shimko, 'Metaphors and Foreign Policy Decision Making' (1994) 15 *Political Psychology* 655 303

Kevin Werbach, 'The Centripetal Network: How the Internet Holds itself Together, and the Forces Tearing it Apart' (2008) 42 *UC Davis Law Review* 343 48

Kevin Werbach, 'The Network Utility' (2011) 60 *Duke Law Journal* 1761 31, 48

Khurram Gore, '*Xiaoning v Yahoo!*: Piercing the Great Firewall, Corporate Responsibility, and the Alien Tort Claims Act' (2008) 27 *Temple Journal of Science, Technology and Environmental Law* 97 306

Kimberlee Weatherall, 'Of Copyright Bureaucracies and Incoherence: Stepping Back from Australia's Recent Copyright Reforms' (2007) 31 *Melbourne University Law Review* 967 160

Kristina Groennings, 'Costs and Benefits of the Recording Industry's Litigation against Individuals' (2005) 20 *Berkeley Technology Law Journal* 571 169

Lauren Patten, 'From Safe Harbor to Choppy Waters: YouTube, the *Digital Millennium Copyright Act*, and a Much Needed Change of Course' (2007) 10 *Vanderbilt Journal of Entertainment and Technology Law* 181 9

Lawrence Lessig, 'The New Chicago School' (1998) 27 *Journal of Legal Studies* 661 28

Lawrence Lessig, 'The Path of Cyberlaw' (1996) 104 *Yale Law Journal* 1743 6

Lawrence Solum and Minn Chung, 'The Layers Principle: Internet Architecture and the Law' (2004) 79 *Notre Dame Law Review* 815 49, 51, 52, 53

Lee Kovarsky, 'A Technological Theory of the Arms Race' (2006) 81 *Indiana Law Journal* 918 12

Marc Aaron Melzer, 'Copyright Enforcement in the Cloud' (2011) 21 *Fordham Intellectual Property, Media and Entertainment Law Journal* 403 13

Marc Galanter, 'Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change' (1974) 9 *Law & Society Review* 95 136

Marius Andreescu, 'Principle of Proportionality, Criterion of Legitimacy in the Public Law' (2011) 18 *Lex ET Scientia* 113 177

Mark Lemley and Lawrence Lessig, 'The End of End-To-End: Preserving the Architecture of the Internet in the Broadband Era' (2001) 48 *UCLA Law Review* 925 51

Mark Lemley and R Anthony Reese, 'Reducing Digital Copyright Infringement Without Restricting Innovation' (2004) 56 *Stanford Law Review* 1345 11

Mark Lemley, 'Rationalizing Internet Safe Harbors' '(2007) 6 *Journal on Telecommunications & High Technology Law* 101 47, 116

Mark Lemley, David Levine and David Post, 'Don't Break the Internet' (2011) 64 *Stanford Law Review Online* 34 21

Mark MacCarthy, 'What Payment Intermediaries Are Doing about Online Liability and Why it Matters' (2010) 25 *Berkeley Technology Law Journal* 1037 41, 46

Michael Boardman, 'Digital Copyright Protection and Graduated Response: A Global Perspective' (2011) 33 *Loyola of Los Angeles International and Comparative Law Review* 223 178

Michael O'Floinn and David Ormerod, 'Social Networking Sites, RIPA and Criminal Investigations' [2011] 10 *Criminal Law Review* 766 59

Michael Rustad and Thomas Koenig, 'Rebooting Cybertort Law' (2005) 80 *Washington Law Review* 335 16, 18, 96

Michael Vogel, 'Unmasking "John Doe" Defendants: The Case against Excessive Hand-wringing over Legal Standards' (2004) 83 *Oregon Law Review* 795 232

Michel Foucault, *About the Beginning of the Hermeneutics of the Self: Two Lectures at Dartmouth* (1993) 21 *Political Theory* 198 187

Nathaniel Gleicher, 'Note — John Doe Subpoenas: Toward a Consistent Legal Standard' (2008) 118 *Yale Law Journal* 320 228

Neal Katyal, 'Criminal law in Cyberspace' (2001) 149 *University of Pennsylvania Law Review* 1003 96

Nic Suzor, 'Privacy v Intellectual Property Litigation: Preliminary Third Party Discovery on the Internet' (2004) 25 *Australian Bar Review* 227 230, 243

Nicolas Suzor and Brian Fitzgerald, 'The Legitimacy of Graduated Response Schemes in Copyright Law' (2011) 34 *University of New South Wales Law Journal* 1

— 163, 175, 177, 178, 181, 186

Olivier Bomsel and Heritiana Ranaivoson, 'Decreasing Copyright Enforcement Costs: The Scope of a Graduated Response' (2009) 6 *Review of Economic Research on Copyright Issues* 13 171, 179

Olivier Bomsel and Heritiana Ranaivoson, 'Decreasing Copyright Enforcement Costs: The Scope of a Graduated Response' [2009] *Review of Economic Research on Copyright Issues* 13 170

Orin Kerr, 'The Problem of Perspective in Internet Law' (2003) 91 *Georgetown Law Journal* 357 8

Patrick van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 *Common Market Law Review* 1455 46

Paul Cox, 'Evolution or Revolution? *Norwich Pharmacal Orders over the Last 20 Years*' (2004) 172 *Trademark World* 40 200

Paul Davies, 'Accessory Liability: Protecting Intellectual Property Rights' [2011] 4 *Intellectual Property Quarterly* 390 40, 70, 74, 89, 92

Peter Birks, 'Rights, Wrongs, and Remedies' (2000) 20 *Oxford Journal of Legal Studies* 1 68

Peter Cane, '*Mens Rea* in Tort Law' (2000) 20 *Oxford Journal of Legal Studies* 533 93

Peter Yu, 'Digital Copyright and Confuzzling Rhetoric' (2011) 13 *Vanderbilt Journal of Entertainment and Technology Law* 881 163

Peter Yu, 'The Graduated Response' (2010) 62 *Florida Law Review* 1374

— 164, 170, 172, 178, 182, 187

Pey-Woan Lee, 'Inducing Breach of Contract, Conversion and Contract as Property' (2009) 29 *Oxford Journal of Legal Studies* 511 70

Philip Hamburger, 'The Development of the Law of Seditious Libel and the Control of the Press' (1985) 37 *Standard Law* Review 661 102, 103

Philip Sales, 'The Tort of Conspiracy and Civil Secondary Liability' (1990) 49 *Cambridge Law Journal* 491 40, 67, 89

R C Donnelly, 'History of Defamation' [1949] *Wisconsin Law Review* 99 136

Randal Picker, 'Copyright as Entry Policy: The Case of Digital' (2002) 47 *Antitrust Bulletin* 423 162

Reinier Kraakman, 'Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy' (1986) 2 *Journal of Law, Economics, and Organization* 53 39, 94

Robert Burrell and Kimberlee Weatherall, 'Exporting Controversy? Reactions to the Copyright Provisions of the US-Australia Free Trade Agreement: Lessons for US Trade Policy' [2008] *Journal of Law, Technology and Policy* 259 12

Robert Burrell, 'Copyright Reform in the Early Twentieth Century: The View from Australia' (2006) 27 *Journal of Legal History* 239 144

Robert LaRose et al, 'Sharing or Piracy? An Exploration of Downloading Behavior' (2005) 11 *Journal of Computer-Mediated Communication* 1 171

Ronald Mann and Seth Belzley, 'The Promise of Internet Intermediary Liability' (2005) 47 *William and Mary Law Review* 239 10, 11, 29, 47, 95, 96

See Hubert Zimmermann, 'OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection' (1980) 28 *IEEE Transactions on Communications* 425 50

Seth Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006) 155 *University of Pennsylvania Law Review* 11 13, 40

Simon Baggs and Rachel Barber, '*A Changing Tide in the Fight against Online Piracy: How Significant is the* Newzbin *Judgment?*' [2010] *Entertainment Law Review* 234 153

Sonia Katyal, 'Filtering, Piracy Surveillance and Disobedience' (2009) 32 *Columbia Journal of Law & Arts* 401 176

Søren Sandfeld Jakobsen, 'Mobile Commerce and ISP Liability in the EU' (2010) 19 *International Journal of Law and Information Technology* 29 85

Stacey Dogan and Mark Lemley, 'Trademarks and Consumer Search Costs on the Internet' (2004) 41 *Houston Law Review* 777 97

Stephan Hagemann and Gottfried Vossen, 'Categorizing User-Generated Content' [2009] *Proceedings of the Web Science* 155 57

Stephen Gilles, 'Negligence, Strict Liability and the Cheapest Cost-Avoider' (1992) 78 *Virginia Law Review* 1291 95

Stuart Paterson and Anna Fitzherbert, 'From Guantanamo Bay to Outer Space: Developments in *Norwich Pharmacal* Relief' (2010) 29 *Civil Justice Quarterly* 38 224

Susan Bright, 'Liability for the Bad Behaviour of Others' (2001) 21 *Oxford Journal of Legal Studies* 311 79

Susan Kiefel, 'Section 92: Markets, Protectionism and Proportionality — Australian and European Perspectives (2010) 36 *Monash University Law Review* 1 178

Thomas Folsom, 'Toward Non-Neutral Principles of Private Law: Designing Secondary Liability Rules for New Technological Uses' (2009) 3 *Akron Intellectual Property Journal* 45 32, 302

Tilman Lüder, 'The Next Ten Years in EU Copyright: Making Markets Work' (2007) 18 *Fordham Intellectual Property, Media & Entertainment Law Journal* 1 143

Tim Wu, 'Tolerated Use' (2007) 31 *Columbia Journal of Law & the Arts* 617 176

Tim Wu, 'When Code Isn't Law' (2003) 89 *Virginia Law Review* 679 7, 13, 97

Timothy Wu, 'Application-Centered Internet Analysis' (1999) 85 *Virginia Law Review* 1163 48

Timothy Wu, 'Copyright's Communications Policy' (2004) 103 *Michigan Law Review* 278 11, 13, 97, 186, 187

Van Vechten Veeder, 'The History and Theory of the Law of Defamation' (1904) 4 *Columbia Law Review* 33 102

Wigmore, 'A General Analysis of Tort-Relations' (1895) 8 *Harvard Law Review* 377 90

Yafit Lev-Aretz, 'Second Level Agreements' (2012) 45 *Akron Law Review* 137 176

Yochai Benkler, 'Freedom in the Commons: Towards a Political Economy of Information' (2003) 52 *Duke Law Journal* 1245 52

Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Common and User Access' (2000) 52 *Federal Communications Law Journal* 561 50

Other secondary sources

Aleksandra Korolova et al, 'Releasing Search Queries and Clicks Privately' (Paper presented at International World Wide Web Conference, Madrid, 20–24 April 2009) 216

Alfred Tennyson, *Aylmer's Field* (1793) 305

Andrés González, 'PayPal and eBay: The Legal Implications of the C2C Electronic Commerce Model' (Paper presented at the 18th BILETA Conference, April 2003, London) 63

Barry Leiner et al, 'Brief History of the Internet' (1995) *Federal Networking Council* 47

Ben Sisario, 'Music Web Sites Dispute Legality of Their Closing' (*The New York Times*, 19 December 2010) 22

Brett Danaher et al, 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France' (January 2012) 170

Brian Carpenter, 'Architectural Principles of the Internet' (1996) (*Internet Engineering Task Force*, RFC 1958) 51

Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (June 2009) 4

Center for Copyright Information, 'What is a Copyright Alert?' (26 February 2013) <http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/> 20

Chris Reed, 'Think Global, Act Local: Extraterritoriality in Cyberspace' (Research Paper No 58/2010, Queen Mary University of London) 16

Commerce Committee, Copyright (Infringing File Sharing) Amendment Bill (119-2) (2010) 170

Communications Alliance Ltd, *A Scheme to Address Online Copyright Infringement* (2011) 20

comScore Inc, *Media Metrix* (October 2011) 58

Consumer Focus, *Response to 'Proposal for Code of Practice Addressing Websites that are Substantially Focused on Infringement'* (19 September 2011) 281

Council of Europe, Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters (Adopted on 26 March 2008) 292

Daphne Keller (Associate General Counsel, Google Europe), Submission to Joint Committee on Privacy and Injunctions, 16 January 2012 (London) 270

Database, Google Inc, 'Web Search Copyright Removal Data' (Copy on file with author, 2 April 2013) 270

David Price, 'Technical Report: An Estimate of Infringing Use of the Internet – Summary' (January 2011) *Envisional Ltd* 141

Department for Business, Enterprise and Regulatory Reform, 'Consultation Document on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing' (July 2008) 164

Department for Business, Innovation and Skills, *Britain's Superfast Broadband Future* (2010) 174

Department for Business, Innovation and Skills, *Consultation Document on Legislation to Address Illicit Peer-to-Peer (P2P) File-Sharing* (16 June 2009) 187

Department for Business, Innovation and Skills, *Digital Economy Act 2010: Impact Assessments* (April 2010) 172, 174

Department for Business, Innovation and Skills, *Impact Assessment for the* Digital Economy Act 2010 (April 2010) 169

Detica, *The Six Business Models for Copyright Infringement* (2012) 278

Eduardo Porter, 'Keeping the Internet Neutral' (*The New York Times*, 9 May 2012) 186

Entertainment Media Research Ltd, *Digital Entertainment Survey* (2008) 170

Entertainment Media Research Ltd, *Digital Entertainment Survey* (2009) 170

European Commission, *Analysis of the Application of Directive 2004/48/EC in the Member States*, SEC(2010) 1589 final 296

European Commission, *Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)* (2011) 218

European Commission, *First Report on the Directive on Electronic Commerce* (2003) 43, 82

European Commission, *Online Services, Including E-Commerce, in the Single Market* (2012) 85, 314

European Commission, *Public Hearing on Directive 2004/48/EC and the Challenges Posed by the Digital Environment* (Brussels, 7 June 2011) 258, 293

European Commission, *Report on the Application of Directive 2004/48/EC* (22 December 2010) 96, 281

European Union Article 29 Data Protection Working Party, Published Opinion 5/2009 on Online Social Networking (12 June 2009) 58

Facebook Inc, 'Report an Unauthorized Photo' (2012) *Help* <http://facebook.com/help/contact/?id=346630525351669> 272

Facebook Inc, 'Reporting a Violation/Infringement of Your Rights' (2012) <http://facebook.com/help/contact/?id=208282075858952> 272

Facebook Inc, 'Terms of Service' (26 April 2011) <http://facebook.com/legal/terms> 271

Frank La Rue, United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (May 2011) 21

Frontier Economics, *Contribution of the Digital Communications Sector to Economic Growth and Productivity in the UK* (2011) 5

Google Inc, 'Autocomplete' (2012) *Inside Search* <http://support.google.com/websearch/bin/answer.py?hl=en&answer=106230> 271

Google Inc, 'Blogger Content Policy' (2012) <http://blogger.com/content.g> 116

Google Inc, 'Controlling Crawling and Indexing' (2012) *Google Developers* <http://developers.google.com/webmasters/control-crawl-index/> 268

Google Inc, 'Follow the Money to Fight Online Piracy' (2 July 2012) *Europe Blog* <http://googlepolicyeurope.blogspot.de/2012/07/follow-money-to-fight-online-piracy.html> 278

Google Inc, 'Google Terms of Service (1 March 2012) <http://google.com/policies/terms/> 116

Google Inc, 'Keeping Personal Information out of Google' (2012) *Help* <http://support.google.com/webmasters/bin/answer.py?hl=en&answer=164133> 270

Google Inc, 'My Removal Requests' (2012) *Webmaster Tools* <http://google.com/webmasters/tools/removals> 270

Google Inc, 'Privacy Policy' (20 October 2011) *Google Privacy Center* <http://www.google.com/intl/en/privacy/privacy-policy.html> 215

Google Inc, 'Removing Content from Google' (2012) *Help* <http://support.google.com/bin/static.py?hl=en&ts=1114905&page=ts.cs> 270

Google Inc, 'Report Other Legal Removal Issue' (2012) *Help* <http://support.google.com/bin/request.py?contact_type=lr_legalother&product=websearch> 270

Google Inc, 'Transparency Report — Removal Requests' (1 April 2013) <http://google.com/transparencyreport/removals/copyright/> 270

Google Inc, 'Transparency Report — User Data Requests' (31 June 2011) <http://google.com/transparencyreport/data/> 190

Google Inc, 'Transparency Report' (31 March 2013) <http://www.google.com/transparencyreport/removals/copyright/> 289

Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth* (2011) 11

Intellectual Property Office, *Transposition Note for Implementation in England and Wales of the IP Directive* (2005) 259

International Federation of the Phonographic Industry, *Digital Music Report* (2012) 17 170

Internet Rights and Principles Coalition, *Charter of Human Rights and Principles for the Internet* (2011) 12

Interview, Anthony House and Dorothy Chou, Policy Directors, Google Inc, 11 May 2012. 270

Interview, Jenni Aldrich, Regional Legal Director, Google Australia Pty Ltd (19 December 2011, Sydney) 224, 242, 293

John Barlow, 'A Declaration of the Independence of Cyberspace' (8 February 1996) <http://projects.eff.org/~barlow/Declaration-Final.html> 6

John Klensin, 'Role of the Domain Name System (DNS)' (2003) (*Internet Engineering Task Force*, RFC 3467) 56

Jonathan Mayer, '"Any Person … a Pamphleteer": Internet Anonymity in the Age of Web 2.0' (7 April 2009) 16

Juniper Research, *Mobile Payment Strategies: Opportunities & Markets 2011–2015* (July 2011) 62

Juvenal, *Satires*, VI 305

Leslie Daigle, 'WHOIS Protocol Specification' (2004) (*Internet Engineering Task Force*, RFC 3912) 56

Letter from Indian Premier League to Twitter Inc, 'Re: Infringement Notification via Twitter Complaint' (21 May 2012) *Chilling Effects* <http://chillingeffects.org/dmca512c/notice.cgi?NoticeID=374943> 272

Lilian Edwards and Charlotte Waelde, 'Online Intermediaries and Liability for Copyright Infringement' (Paper presented at the World Intellectual Property Organization, Geneva, 2005) 8, 33

Mark MacCarthy, 'Deleting Commercial Pornography Sites from the Internet: The US Financial Industry's Efforts to Combat this Problem' (Evidence to House Committee on Energy and Commerce, 2006) 63

MarkMonitor, *Traffic Report: Online Piracy and Counterfeiting* (January 2011) 59

Martin Kretschmer et al, 'Statement on Constitutional Aspects of the Digital Economy Bill' (1 April 2010) 178

McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011) 5, 317

Michael Meyer, 'Crimes of the "Net"' (13 November 1994, *Newsweek*, New York) 7

Michael Piatek, Tadayoshi Kohno and Arvind Krishnamurthy, 'Challenges and Directions for Monitoring P2P File Sharing Networks — or Why My Printer Received a DMCA Takedown Notice' (Paper presented at 3rd USENIX Workshop on Hot Topics in Security, San Jose, 29 July 2008) 175

Michael Piatek, Tadayoshi Kohno and Arvind Krishnamurthy, *Challenges and Directions for Monitoring P2P File Sharing Networks: or — Why My Printer Received a DMCA Takedown Notice* (2008) 229

Microsoft Corporation, 'Bing Content Removal' (2012) <http://support.discoverbing.com/eform.aspx?productKey=bingcontentremoval> 271

National Audit Office, *Government on the Internet: Progress in Delivering Information and Services Online* (13 July 2007) 4

New South Wales Law Reform Commission, *Report 75 — Defamation* (1995) <http://www.lawlink.nsw.gov.au/lrc.nsf/pages/R75CHP9> 125

New Zealand Federation Against Copyright Theft, 'One Warning Will Stop Most Youth from Infringing Movies Online' (Press Release, 20 October 2009) 170

Nicola Lucchi, 'Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI)' (Unpublished paper no 11-07, 2010) 181

OECD, *Online Payment Systems for E-Commerce* (2006) 62, 63

OECD, *Participative Web: User-Created Content* (12 April 2007) DSTI/ICCP/IE(2006)7/FINAL 57

OECD, *The Economic and Social Impact of Electronic Commerce* (1999) 7

OECD, *The Economic and Social Role of Intermediaries* (2010) 47

OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives* (2011) 47, 183

OFCOM, *'Site Blocking' to Reduce Online Copyright Infringement* (May 2011) 21, 280, 284

Office for National Statistics, *Internet Access — Households and Individuals* (31 August 2011) 4

OpenNet Initiative, 'YouTube and the Rise of Geolocational Filtering' (13 March 2008) <http://opennet.net/blog/2008/03/youtube-and-rise-geolocational-filtering> 311

Optify Inc, *The Changing Face of SERPs: Organic Click Through Rate* (2011) 258

Paul Cornish et al, *Cyber Security and the UK's Critical National Infrastructure* (September 2011) 4

Paul Mockapetris, 'Domain Names — Concepts and Facilities' (1987) (*Internet Engineering Task Force*, RFC 1034) 56

PayPal Inc, 'Financials' (January 2012) *PayPal Press Center* <https://paypal-media.com/about> 62

Peter Hustinx, 'Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)' (22 February 2010) 182

Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines (Adopted 4 April 2012) 287

Richard Clayton, 'Failures in a Hybrid Blocking System' (Paper presented at Workshop on Privacy Enhancing Technologies, Dubrovnik, 30 May 2005) 283

Robert Layton and Paul Watters, 'Investigation into the Extent of Infringing Content on BitTorrent Networks' (April 2010) *Internet Commerce Security Laboratory* <http://afact.org.au/research/bt_report_final.pdf> 142

Sandvine Inc, *Global Internet Phenomena Report* (2012) 142

Sara Radicati (ed), *Email Statistics Report, 2011–2015* (May 2011) 4

Sophocles, *Antigone* (2003 ed, Reginald Gibbons and Charles Segal trans) 14

Sylvain Dejean, 'Une Première évaluation des Effets de la loi Hadopi sur les Pratiques des Internautes Français' (March 2010) 170

Sylvain Dejean, Thierry Penard and Raphaël Suire, 'The French "Three Strikes Law" against Digital Piracy and the Change in Usages of Pirates' (Paper presented at Internet, Politics, Policy 2010, Oxford, 16 September 2010) 173

The Economist Newspaper Ltd, 'Reaching for the Kill Switch' (*The Economist*, 10 February 2011) 23

Timothy Endicott, 'Proportionality and Incommensurability' (Unpublished draft) (2012) 226

Tom Zeller, 'Times Withholds Web Article in Britain' (*The New York Times*, 29 August 2006) 8

United Nations Special Rapporteur on Freedom of Opinion and Expression et al, *Joint Declaration on Freedom of Expression and the Internet* (1 June 2011) 309

USC Annenberg Innovation Lab, *Ad Transparency Report* (5 January 2013) 274

Verizon Communications Inc, *2012 Data breach Investigations Report* (2012) 16

Visa Inc, *Annual Report 2011* (2011) 62

William Dutton and Grant Blank, *Next Generation Users: The Internet in Britain* (2011) 4, 267

William Shakespeare, *The Tragedy of Coriolanus* (1608) 14

World Intellectual Property Organization, 'Case Outcome by Year(s) (Breakdown)' (2012) *Arbitration and Mediation Center* <http://wipo.int/amc/en/domains/statistics/outcome.jsp> 171

World Intellectual Property Organization, Standing Committee on Copyright and Related Rights (4–8 November 2002) SCCR/8/2 40

Yahoo! Inc, 'What are Content Filters?' (2012) *Flickr FAQ* <http://flickr.com/help/filters/> 311

Yana Breindl and François Briatte, 'Digital Network Repertoires and the Contentious Politics of Digital Copyright in France and the European Union' (Paper presented at the Oxford Internet Institute conference, Oxford, 16 September 2010) 163

YouTube LLC, 'Content ID' (2011) <http://www.youtube.com/t/contentid> 59

YouTube LLC, 'YouTube Community Guidelines' (2010) <http://youtube.com/t/community_guidelines> 58