New Dimensions in Privacy Law

International and Comparative Perspectives

Edited by **Andrew T. Kenyon** and **Megan Richardson**

CAMBRIDGE

CAMBRIDGE www.cambridge.org/9780521860741

This page intentionally left blank

NEW DIMENSIONS IN PRIVACY LAW

This broad-ranging examination of privacy law considers the challenges faced by the law in changing technological, commercial and social environments. It encompasses three overlapping areas of analysis: privacy protection under the general law; legislative measures for data protection in digital communications networks; and the influence of transnational agreements and other pressures toward harmonised privacy standards. Leading, internationally recognised authors discuss developments across these three areas in the United Kingdom, Europe, the United States, APEC (the forum for Asia-Pacific Economic Cooperation), Australia and New Zealand. Chapters draw on doctrinal and historical analysis of case law, theoretical approaches to both freedom of speech and privacy, and the interaction of law and communications technologies, in order to examine present and future challenges to law's engagement with privacy.

Andrew T. Kenyon is the Director of the Centre for Media and Communications Law at the University of Melbourne, and Associate Professor in the Faculty of Law. He researches in comparative media law, across topics in defamation, privacy, journalism, media regulation and copyright. These interests come together in his role as editor of the refereed international journal, the *Media & Arts Law Review*.

Megan Richardson is the Deputy Director of the Centre for Media and Communications Law at the University of Melbourne, and Associate Professor in the Faculty of Law. Her research spans the fields of intellectual property and privacy.

NEW DIMENSIONS IN PRIVACY LAW

INTERNATIONAL AND COMPARATIVE PERSPECTIVES

Edited by

ANDREW T. KENYON

AND

MEGAN RICHARDSON

Centre for Media and Communications Law
Faculty of Law
University of Melbourne

CAMBRIDGE
UNIVERSITY PRESS

cambridge university press
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge cb2 2ru, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521860741

First published in print format 2006

isbn-13 978-0-511-25654-7 eBook (EBL)
isbn-10 0-511-25654-X eBook (EBL)

isbn-13 978-0-521-86074-1 hardback
isbn-10 0-521-86074-1 hardback

CONTENTS

CONTRIBUTORS

Eric Barendt, Goodman Professor of Media Law, Faculty of Laws, University College London, United Kingdom.

J. Marc Dinant, Computer Scientist, Senior Lecturer at the University of Namur, Belgium; Expert to the Article 29 Working Party of the European Commission.

Graham Greenleaf, Professor, Faculty of Law, University of New South Wales, Australia; Co-Director, Australasian Legal Information Institute.

Lesley Hitchens, Senior Lecturer, Faculty of Law, University of New South Wales, Australia.

Kenneth J. Keith, Member of the International Court of Justice; Judge of the Supreme Court of New Zealand; Professor Emeritus, Victoria University of Wellington, New Zealand.

Andrew T. Kenyon, Director, Centre for Media and Communications Law, and Associate Professor, Faculty of Law, University of Melbourne, Australia.

David Lindsay, Senior Lecturer, Faculty of Law, Monash University, Australia.

Brian C. Murchison, Charles S. Rowe Professor of Law, Washington and Lee University School of Law, Virginia, United States.

Gavin Phillipson, School of Law, King's College London, United Kingdom.

Yves Poullet, Dean, Faculty of Law and Director of the Centre de Recherche Informatique et Droit, University of Namur, Belgium.

Megan Richardson, Associate Professor, Faculty of Law, University of Melbourne, Australia.

Sam Ricketson, Professor, Faculty of Law, University of Melbourne, Australia; Barrister, Victoria, Australia.

Raymond Wacks, Emeritus Professor of Law and Legal Theory, University of Hong Kong.

PREFACE

It has been a tremendous pleasure to work with leading academic and judicial figures from five countries in producing this collection which addresses issues in UK, European, US, Australian, New Zealand and Asian privacy law. This project began with an Australian Research Council discovery grant on privacy and the internet, awarded to Sam Ricketson, Megan Richardson and Lesley Hitchens, and then took on a life of its own. A series of public seminars on 'Privacy: New Issues and Policies' was presented under the auspices of the CMCL – Centre for Media and Communications Law – at the University of Melbourne during 2003 and 2004. We are grateful to the Law School and the sponsors of the CMCL for their support of the events, and to the administrative staff at the CMCL who make such seminars run so smoothly.

After the seminar series, we commissioned further chapters to increase the collection's breadth and depth, as well as developing all the chapters with their authors. Thanks to Cambridge University Press for their enthusiastic support for this publication as well as to two anonymous referees who gave some most helpful insights and suggestions on our original proposal. We also appreciate the contributions of Martin Vranken, in translating the chapter by Yves Poullet and Marc Dinant, and of Kate MacNeill and Jason Bosland at the CMCL for their assistance during the editing phase. Above all, thanks to the authors for their thoughtful chapters and careful revisions, and for their thorough engagement with the project throughout.

Andrew Kenyon and Megan Richardson
Melbourne, January 2006

1

New dimensions in privacy: Communications technologies, media practices and law

ANDREW T. KENYON AND MEGAN RICHARDSON

While the idea of 'privacy' is venerable,[1] modern obsessions with privacy are largely rooted in the twentieth century, particularly the years following the Second World War. The precise reasons may vary and change over time. As any European civilian lawyer will confirm, the European Convention on Human Rights,[2] with its important provision for security of private life alongside its protection of freedom of expression,[3] was a direct response to the many and varied intrusions on personal integrity that occurred during the war years. In Europe it still represents a bulwark against organised authority, and significantly not only one limited to the authority of the state.

An American lawyer would almost certainly refer to the paradigmatic work of Warren and Brandeis,[4] which preceded the twentieth century by only a few years, and its later revision by Prosser.[5] However, such a lawyer might well add that the human rights movement of the 1960s and 1970s really established the modern conception of rights as basic to a democratic polity in the United States – even if it was free speech rather than privacy that emerged as dominant. The rights had to contend for success in America's so-called 'marketplace of ideas',[6] and the competition

[1] Authorities cited for the word 'Privacy' in the *Oxford English Dictionary Online* (Oxford: Oxford University Press, 1989–2005) date back to the early seventeenth century and before.

[2] Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952).

[3] Ibid. Article 8 and Article 10 respectively.

[4] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193. Indeed not only American lawyers commonly cite this – and it is referred to in the OED, above n.1, as authority for 'privacy' as 'The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right'.

[5] William L. Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

[6] In the words of Holmes J (dissenting) in *Abrams* v. *United States*, 250 US 616 at 630 (1919) 'that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out . . . is the theory of our Constitution'.

was prefigured by the First Amendment's explicit reference to freedom of expression as a basic American value and the interpretation of that constitutional wording by courts, particularly since the 1960s.[7] Here at least there is some basis for difference with the rest of the world.[8]

English lawyers might observe that privacy has been part of the fabric of English law since at least the case of *Entick* v. *Carrington*,[9] but sometimes find it difficult to explain emerging concerns about privacy except as a European phenomenon swept to England under the impetus of the European Convention. Such an analysis, however, underplays the technological and commercial developments that have led to new pressures for privacy protection. And it arguably neglects ongoing domestic debates about media practices, which are longstanding and have often been linked to the roles of self-regulatory bodies like the Press Complaints Commission.[10] While the European influence is real and of undoubted significance, there is also a certain prosaic utilitarianism to contemporary English legal discussions about privacy, which suggests a distinction from the dignitarian rights-based approaches of continental Europe. If England can be seen as the first home of utilitarianism, it can also be acknowledged that while utilitarians might use the language of rights their ultimate concerns are with social welfare: the 'greatest happiness for the greatest number', as put by Jeremy Bentham and John Stuart Mill.[11]

[7] See, e.g., *New York Times* v. *Sullivan*, 376 US 254 (1964); *Time Inc.* v. *Hill*, 385 US 374 (1967); Melville B. Nimmer, 'The Right to Speak From *Times* to *Time*: First Amendment Theory Applied to Libel and Misapplied to Privacy' (1968) 56 *California Law Review* 935.

[8] See, e.g., Frederick Schauer, 'The Exceptional First Amendment' in Michael Ignatieff (ed.), *American Exceptionalism and Human Rights* (Princeton: Princeton University Press, 2005) p. 29.

[9] *Entick* v. *Carrington* (1765) 19 St Tr 1029.

[10] See, e.g., United Kingdom, Home Office, *Report of the Committee on Privacy and Related Matters*, Cm 1102 (London: HMSO, 1990) (commonly known as the '*Calcutt Report*'); Raphael Cohen-Almagor, *Speech, Media and Ethics: The Limits of Free Expression* (Basingstoke, UK: Palgrave, 2001) chap. 7 'The Work of the Press Councils . . .' and particularly pp. 124–32 for a review of the UK history, preceding and following the *Calcutt Report*, and the influence of concerns about press intrusion in UK debates; David Sherborne and Sapna Jethani, 'The Privacy Codes' in Michael Tugendhat and Iain Christie (eds.), *The Law of Privacy and the Media* (Oxford: Oxford University Press, 2002) chap. 13 and *First Cumulative Updating Supplement* (2004); and Russell L. Weaver, Andrew T. Kenyon, David F. Partlett and Clive P. Walker, *The Right to Speak Ill: Defamation, Reputation and Free Speech* (Durham, NC: Carolina Academic Press, 2006) pp. 124–7 and p. 273 for details about the pattern of complaints to the Press Complaints Commission in recent years.

[11] Although Mill at least attempted to acknowledge rights as entailing 'vastly more important, and therefore more absolute and imperative' social utilitites: 'Utilitarianism' in John Stuart

Those in former English colonies such as Australia and New Zealand seem more conflicted in attitudes to privacy. Our debates about privacy and free speech appear as pale companions to English battles between celebrities seeking to control personal revelations (with one eye to preserving a marketable reputation) and the media whose business includes celebrity revelation.[12] There may be less concern than in our European counterparts with founding rights on notions of personal integrity; although we may readily say that privacy is about dignity as much as utility, there is a sense that we do not hold to this when it comes to providing special legal support.[13] And although we may reference freedom of speech we are more cynical than American lawyers about claims as to its fundamental political importance in the development of an autonomous subject. Concerns about public security offer another reason to limit privacy, as do the market imperatives of commerce: in Australia the force of arguments from security or markets may be even stronger than arguments from free speech. But here Australia does not stand apart from much of the world, except perhaps in the degree of emphasis. There are other countries too, for instance in Asia, where in a conflict with commerce or security privacy may not count for much. In any event, recent international trends appear to be going against privacy in relation to issues of safety: until recently it might have been said in many western societies that protection of public security could rarely justify severe encroachments on privacy – notwithstanding concerns about uses of data surveillance

Mill, *Utilitarianism, On Liberty and Essay on Bentham*, ed. and intro. Mary Warnock (London: Collins, 1962) p. 321. This position can be critiqued as incoherent, but it does provide a pragmatic mechanism for accommodating the language of rights within what is still an essentially utilitarian framework. See further Megan Richardson, 'Whither Breach of Confidence: A Right of Privacy for Australia?' (2002) 26 *Melbourne University Law Review* 381 at 391–3 especially.

[12] Perhaps it is the UK that is unusual. In 2005, *The Economist* reported that 'Britons buy almost half as many celebrity magazines as Americans do, despite having a population that is only one-fifth the size' and '[n]ew figures from the Audit Bureau of Circulation show that the ten best-selling celebrity publications and ten most popular tabloids have a combined circulation of 23m': 'Making and Marketing Celebrities: The Fame Machine' (2005) 376 (8442) *The Economist* 49 (3 September).

[13] This is particularly clear in the minimal implementation given in Australia to the data protection standards required under the European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995, *OJ*, L 281, 23 November 1995 (which requires countries outside the EU to provide adequate protection to personal information in order for data to move freely to them from EU states): see Privacy Act 1988 (Cth) (especially 2000 amendments).

technologies[14] – but this position faces multiple challenges from current political and public perceptions.

This collection encompasses three overlapping areas of analysis: issues about privacy protection under the general law, legislative measures affecting privacy that are aimed at data protection within digital communications networks, and the influences of transnational agreements and other pressures toward harmonised standards. The issues of general law can be related to transforming communications technologies and media practices. The issues of legislative measures, at least those aimed at data protection within digital communications networks, are connected with the transactions of individuals, as citizens and consumers, with state and commercial actors. And the pressures for harmonisation of laws are related in part to the changing authorities of nation states and the emergence of new legal organisations and communities of influence, particularly linked with international trade and the internet.[15] The various authors in this book explore these issues, offering insights that have general as well as comparative interest.

That freedom of speech and privacy are not always in conflict is the message of Eric Barendt in chapter 2. Barendt reviews and revises the 'standard theme' that privacy and speech conflict such that one must prevail over the other; and observes that speech includes private as well as public expression. Thus where the protection of private speech is in issue, the dilemma faced in legal cases, sometimes explicit but more often implicit, is not so much privacy *versus* free speech as which *kind* of speech should be privileged. The analysis suggests that the values associated with privacy and expression may not be as distinct as commonly supposed. On the one hand, privacy is not just the right 'to be let alone' – the classic Warren and Brandeis view[16] – but includes private interchanges and shared experiences within non-public communities. On the other hand, expression is not simply about what goes on in public arenas; freedom of expression includes choices as to mode, timing, location, audience – whether public or private – and even the choice not to speak at all if expression is understood as a freedom connected to liberty and autonomy. These points about privacy's social dimensions are picked up in the third chapter by our American contributor, Brian Murchison, who argues that selective

[14] See, e.g., Cees J. Hamelink, *The Ethics of Cyberspace* (London, Sage, 2000).

[15] See, e.g., John Braithwaite and Peter Drahos, *Global Business Regulation* (Cambridge; Cambridge University Press, 2000); Kathy Bowrey, *Law and Internet Cultures* (Cambridge: Cambridge University Press, 2005).

[16] Warren and Brandeis, 'The Right to Privacy', above n. 4 at 205.

sharing of private personal matters is a means to forge close relationships based on trust, drawing in particular on the work of Richard Rorty – and his use of Sigmund Freud, Ralph Waldo Emerson, John Dewey and others[17] – and on the work of Charles Taylor.[18] The chapter suggests the importance of maintaining that freedom should not be underestimated in a society that places high value on free speech, and examines a number of recent cases in which American courts seem sympathetic to such ideas, notwithstanding the breadth taken by the courts in construing a 'matter of legitimate public concern'.[19] While Murchison's focus is largely on media publicity, envisaging the self as a 'web of relations'[20] has implications for later chapters including those focused on digital communications, data protection and Digital Rights Management (DRM) systems. In addition, non-US readers may be struck by the presence of the jury as an element in analysing US privacy protection under its general law. This jury role is necessary given US federal and state constitutional provisions,[21] but is surely a notable difference which should influence how evaluations of privacy protection seek to draw comparatively on US experiences.[22]

Clearly, 'public' as well as 'private' may have many meanings. Public expression does not necessarily entail instantaneous communication to the entire world any more than private expression necessarily entails an audience of only one. In the past what was called 'public expression' was typically directed to a particular audience (albeit bigger or different from the audience that the privacy subject would have chosen) and publication was often of a rather transitory nature, at least in terms of the audience's practical ability to access the material. In such cases, privacy interests may not have seemed all that much imperilled if unwanted publication occurred without the possibility of legal recourse. But the concern is greater for networked publications, crossing physical national boundaries

[17] See, e.g., Richard Rorty, *Contingency, Irony, and Solidarity* (Cambridge: Cambridge University Press, 1989); Richard Rorty, *Philosphy and Social Hope* (London: Penguin, 1999).

[18] Charles Taylor, *The Ethics of Authenticity* (Cambridge, Mass.: Harvard University Press, 1992).

[19] See *Restatement (Second) of Torts* (St Paul, Minn.: American Law Institute, 1977) s. 625D.

[20] Rorty, *Philosophy and Social Hope*, above n. 17 at 53.

[21] The US federal Constitution's Seventh Amendment provides for a right to jury trial for all claims above $20; most state Constitutions provide similar rights. See *Colgrove* v. *Battin*, 413 US 149 (1973).

[22] The presence of juries in both defamation and privacy litigation in the US is a contrast to the situation in, e.g., England where the jury role extends only to defamation; see, e.g., Andrew T. Kenyon, *Defamation: Comparative Law and Practice* (London: UCL Press, 2006).

and generally being stored and accessible in various forms over long periods. Potential risks raised by the internet, and various attempts to address them at the European level, are canvassed in chapter 4 by Yves Poullet and Marc Dinant. In a close analysis of the network's open character as well as its opaque qualities – such as, the lack of transparency to users that can exist with targeted advertising, differential pricing, limited access to particular sites, and search engines – they seek to clarify and resolve debates about the internet's implications for privacy. Investigating legislative and market-based approaches that may be suitable for the situation where information flows and surveillance are facilitated *together*, they would go further than current provisions in framing a charter of privacy principles aimed at increasing the control which data subjects can exercise over their own circumstances. As Terry Flew notes, the network poses 'a paradoxical scenario' in that consumers are seen as gaining 'voice' in the market, but only through 'willingly divulg[ing] information about their preferences as consumers'.[23] There is another aspect to this chapter – it shows how privacy standards within national jurisdictions may be strongly affected by regional standards, in this case within the EU. Similarly, regional privacy issues are canvassed in chapter 5 for the Asia-Pacific region. Graham Greenleaf examines the APEC Privacy Framework[24] – the most significant recent transnational instrument on privacy – within the context of existing European and US approaches to privacy protection. Usefully reviewing the history of the Framework's development, he sets out how its privacy principles adopt a low standard of protection, whether in comparison to existing international instruments or regional national laws, and raises serious issues for the implementation of the Framework. Like Poullet and Dinant's proposals, the analysis is tempered by realism about the constraints legislators feel when privacy intersects with other interests, especially in relation to commerce, public security and, in some ways at least, freedom of speech.

Interests in intellectual property provide another source of potential constraint, which is the focus of chapter 6 by David Lindsay and Sam Ricketson. They outline the matters at stake in the conjunction of DRM systems and privacy – an issue that can be expected to pose significant future policy questions. Superficially, of course, privacy and intellectual property have a great deal in common. Both almost invariably concern information. Both involve preserving a degree of individual control and

[23] Terry Flew, *New Media: An Introduction* (2nd edn, South Melbourne: Oxford University Press, 2005).

[24] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, November 2004; available from http://www.apec.org/.

ability to exclude in the face of a public desire for access. Both may be explained and justified in utilitarian as well as dignitarian policy terms. And, as the authors suggest, these policy terms reflect different understandings of the relation between law and the market. Lindsay and Ricketson outline ways in which both economic analysis and consideration of non-market-based values will be important in framing regulatory approaches to DRM systems – with a keen understanding of the possibilities for those approaches to draw on technology as well as on law.

Many of the recent developments in privacy law have concerned not legislation, or not *simply* legislation, but law as developed in cases during the last half decade – particularly in England, New Zealand and the European Court of Human Rights. The final chapters in this book consider the vexed question of how courts should go about protecting privacy when the legislature has not provided clear guidance. The issue is not simply whether a privacy tort or torts would be preferable to reliance on more traditional doctrines – a development suggested, for example, by Sedley LJ in *Douglas* v. *Hello! Ltd.*[25] As Murchison's analysis shows, privacy torts are common in US courts, but questions still exist as to whether sufficient recognition is given to privacy interests to address contemporary social values. Rather debates about privacy and the general law encompass the question of whether courts in common law jurisdictions go far enough in reflecting privacy values in their legal decisions. The contributions offer some unique insights. In chapter 7, Raymond Wacks contends that generally conservative English courts are not very interested in implementing what they see as European-style privacy norms and, if anything, have used doctrines such as breach of confidence as a panacea for the inadequate protection of privacy. In a somewhat different interpretation, Gavin Phillipson in chapter 8 suggests that English courts have effectively adapted breach of confidence into a de facto privacy tort offering a greater scope for privacy protection than before, but adds that they face difficulties now as the level of privacy protection demanded by the European Court of Human Rights appears to have expanded markedly in recent jurisprudence.[26] Might it almost be getting to the stage that, as lawyer and journalist Joshua Rozenberg has predicted, 'anyone photographed at a public event ha[s] the right to veto an unflattering shot'?[27] In chapter 9 our New Zealand contributor, Sir Kenneth Keith, suggests that, irrespective of whether a tort of privacy is adopted (and New Zealand courts

[25] *Douglas* v. *Hello! Ltd* [2001] QB 967 at para. 126.
[26] See *Von Hannover* v. *Germany* (2005) 40 EHRR 1.
[27] Joshua Rozenberg, *Privacy and the Press* (revised edn, Oxford: Oxford University Press, 2005), p. xvi.

have indeed moved in this direction),[28] courts need to be wary about offering broad support for privacy where the legislature has not elected to do so, especially given this is an area where there has now been considerable legislation. In the concluding chapter, Megan Richardson and Lesley Hitchens take as their starting point the historical role of courts in developing traditional doctrines to serve new situations and circumstances, and examine the treatment of breach of confidence and related doctrines in the nineteenth-century celebrity privacy case of *Prince Albert* v. *Strange*.[29] The conclusion drawn is that not only are there surprising factual parallels to be drawn between this case and modern celebrity privacy cases but the reasoning in the nineteenth-century judgments shows an awareness that, notwithstanding the potential exchange value associated with a celebrity's image, the choice instead to maintain a degree of privacy can be defended in utilitarian terms as integral to individual flourishing and social development, ideas brought out further in the writings of John Stuart Mill.[30]

The chapters in this book take different approaches to their subjects – for example Murchison analyses recent US cases and substantial literature from outside law to consider possible doctrinal change to US privacy torts; Wacks and Barendt draw on their own developed philosophical positions on privacy and free speech; Richardson and Hitchens' focus is essentially historical; Poullet and Dinant, Greenleaf, and Lindsay and Ricketson pay close attention to the interaction of technology and law; Keith provides a useful judicial perspective; while Phillipson provides a close doctrinal analysis of contemporary English and European legal judgments. Within this variety of interests and of methods, some themes recur across the broad issues of protecting privacy under case law, legislating for data protection in digital networks, and the roles of transnational agreements and influences of pressures for harmonised standards: for example, that private and public are relative concepts; that technology can radically change the landscape on which laws are made; that in this area questions

[28] The history of the tort approach in New Zealand, and its most recent enunciation by the Court of Appeal in *Hosking* v. *Runting* [2005] 1 NZLR 1, is set out in John Burrows and Ursula Cheer, *Media Law in New Zealand* (5th edn, South Melbourne: Oxford University Press, 2005) pp. 245ff. See also Megan Richardson, 'Privacy and Precedent: The Court of Appeal's Decision in Hosking v Runting' (2005) 11 *New Zealand Business Law Quarterly* 82.

[29] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652; 64 ER 293 and (1849) 1 H & TW 1; 47 ER 1302.

[30] See, e.g., 'On Liberty', in John Stuart Mill, *Utilitarianism, On Liberty and Essay on Bentham*, above n. 11 at pp. 126–250.

of law and theory appear to be inextricably linked; and perhaps that the scope for national differences may be reducing. Of course, none of these recurring themes should be thought of as supporting commonplace, if somewhat misleading, arguments about digital communications driving revolutions in social, political and economic practices and sidelining the role of the state.[31] The changes are more nuanced, and the times are less revolutionary, as this volume seeks to suggest in its exploration of new dimensions in privacy law.

In doing so, the book lays a base for future privacy research. No doubt there will be more legislative developments and judicial decisions to be discussed (including an anticipated appeal to the House of Lords in the *Hello!* case). Beyond these, more consideration might be made of media production practices and the role, if any, that privacy law plays within the decisions of journalists, editors and producers and their legal advisers.[32] There might also be more substantial efforts to engage with contemporary issues of production, circulation and consumption of celebrity identity, and the interpenetrations of media and celebrity industries in the production of celebrity content.[33] The contested social roles of popular media content deserve examination. Some contemporary and historical instances suggest mediated 'gossip' about formerly private matters has reshaped public spheres in more inclusive forms that suggest notable political potential in such media content.[34] But some such practices are decried as merely being 'tabloidisation' – at times inflected by non-explicit judgments of taste or class[35] – and linked to questions about the ethics

[31] See further, e.g., Christopher May, *The Information Society: A Sceptical View* (Cambridge: Polity, 2002).

[32] Existing research into defamation law and the media could provide useful models for such research endeavours; see, e.g., Weaver et al., above n. 10; Chris Dent and Andrew T. Kenyon, 'Defamation Law's Chilling Effect: A Comparative Content Analysis of Australian and US Newspapers' (2004) 9 *Media & Arts Law Review* 89; and Kenyon, *Defamation*, above n. 22, chap. 1 for an overview of other empirical research in the field.

[33] Useful starting points from varied theoretical perspectives could include Graeme Turner, *Understanding Celebrity* (London: Sage, 2004); John B. Thompson, *Political Scandal: Power and Visibility in the Media Age* (Cambridge: Polity Press, 2000); Graeme Turner, Frances Bonner and P. David Marshall, *Fame Games: The Production of Celebrity in Australia* (Melbourne: Cambridge University Press, 2000); Catherine Lumby, *Gotcha: Life in a Tabloid World* (St Leonards, NSW: Allen & Unwin, 1999).

[34] See, e.g., Alan McKee, *The Public Sphere: An Introduction* (Cambridge: Cambridge University Press, 2005) pp. 32–42 and *passim*.

[35] For a review of arguments about tabloidisation, drawing on primarily UK and Australian examples, see Graeme Turner, *Ending the Affair: The Decline of Television Current Affairs in Australia* (Sydney: University of NSW Press, 2005) chap. 3. Some of the material that

of media practices.[36] However, here we are moving beyond the particular project of this book. It is enough that the collective contributions represent an important transition towards a sophisticated, multidimensional treatment of contemporary privacy issues. More could also be said about each of the chapters, but even a longer introduction could not hope to do justice to their richness and complexities. For a fuller appreciation we commend them to your reading.

Turner uses can be updated by reference to the UK regulator Ofcom's investigation of public service broadcasting; see, e.g., United Kingdom, Ofcom, *Ofcom Review of Public Service Television Broadcasting: Phase 2 – Meeting the Digital Challenge* (London: Ofcom, 2004) and more recent documents in the review available from www.ofcom.org.uk.

[36] See, further, Catherine Lumby and Elspeth Probyn (eds.), *Remote Control: New Media, New Ethics* (Cambridge: Cambridge University Press, 2003).

2

Privacy and freedom of speech

ERIC BARENDT

Introduction

There is a vast amount of literature both on privacy and on freedom of speech and of the press as discrete constitutional and legal rights. Moreover, the relationship between them has been explored in a number of books and law review articles.[1] But now the advent of novel electronic technologies for communication gives a fresh impetus to the discussion and invites reconsideration of a familiar theme. Simply stated, this theme is that privacy rights and interests inevitably conflict with the right to freedom of speech (or expression). A standard argument is that the right to control the dissemination of personal information may be trumped by the interest of the public in knowing private, even intimate, facts about politicians, public officials, or celebrities, because the public has a right to know the truth about such people. On the other hand, it can be contended that freedom of speech does not even cover private gossip, since gossip is not worthy of protection under any clause guaranteeing the right to free speech. And even if freedom of speech does cover the disclosure of private or personal information, it does not protect it from legal action in every case; the two rights or interests have to be balanced and weighed in the context of the particular facts. The point is that there is always a clash of rights, which must be resolved either in favour of the privacy right or of the right to freedom of speech.

In this chapter I want to make a limited challenge to this traditional perspective concerning the relationship of these two fundamental rights. I will argue that in some situations the two rights do not conflict. Rather, the protection of privacy is often essential to freedom of speech, at least

[1] E.g., see Raymond Wacks, *Privacy and Press Freedom* (London: Blackstone Press, 1995); Eric Barendt, 'Privacy and the Press' in Eric M. Barendt (ed.), *Yearbook of Media and Entertainment Law 1995* (Oxford: Clarendon Press, 1995) pp. 23–41; Basil S. Markesinis (ed.), *Protecting Privacy* (Oxford: Oxford University Press, 1999).

insofar as that freedom is understood to refer to the freedom of personal communication between two individuals or among a small group of people. This point is particularly pertinent in the context of electronic communications by the internet, although it is certainly not confined to them. There are other contexts in which privacy and freedom of speech go hand in hand, rather than conflict. But of course there are cases of conflict, and I say something about those cases before turning to others, where it will be suggested that we need to look at the relationship of the two rights differently.

A few introductory remarks should be made before we examine these two categories of case. Privacy is an elusive concept, so elusive in fact that it has generally proved impossible for Australian and English lawyers to discover its exact whereabouts in the common law. The Human Rights Act 1998 came into force in the United Kingdom in October 2000. It incorporates into UK law the right to respect for private life guaranteed by Article 8 of the European Convention on Human Rights (ECHR), as well as the freedom of expression guaranteed by Article 10.[2] Many lawyers thought an inevitable result of incorporation would be that English law would at last recognise the right to privacy, overcoming the reluctance of the common law.[3] The Court of Appeal has, however, refused to take that step, notably in *A* v. *B plc*,[4] when a Premier League footballer unsuccessfully attempted to stop a Sunday newspaper disclosing details of his two casual extra-marital affairs. Lord Woolf CJ preferred to resolve the case on the well-established principles of breach of confidence, and held that the public had an interest in reading about the private life of a figure who for many readers was a 'role model'. Further, in *Wainwright* v. *Home Office*,[5] which concerned the strip-searching of the claimant and her son before visiting another son in prison, the House of Lords rejected the argument that English common law now recognised a tort of privacy. In the leading speech Lord Hoffmann considered it would be unwise for the courts to formulate a 'high-level right to privacy'; in his view there was a distinction between the value of privacy, which might influence the development of the law, and privacy as a legal principle or actionable right.[6]

[2] Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952).

[3] Strong judicial support for this view was expressed by Sedley LJ in the first 'privacy' case to come to the courts after the Human Rights Act came into force in October 2002: *Douglas* v. *Hello! Ltd* [2001] QB 967 at para. 126.

[4] [2003] QB 195.

[5] [2004] 2 AC 406. The facts arose before the Human Rights Act came into force, so reliance could not be placed on the Convention right to privacy.

[6] *Wainwright* v. *Home Office* [2004] 2 AC 406 at paras. 18–31.

The most important recent decision is that of the House of Lords in *Campbell* v. *MGN Ltd.*[7] Naomi Campbell brought proceedings when the *Daily Mirror* had published a number of articles revealing that she was receiving treatment at Narcotics Anonymous (NA) for drug addiction; they disclosed details of the treatment and were accompanied by pictures of the supermodel leaving a meeting of NA. By a bare majority, the House of Lords upheld the claim that the publications infringed her privacy, but both Lord Hope and Baroness Hale, in the leading speeches for the majority, emphasised that the privacy interest was protected by an action for breach of confidence.[8] In short, the courts in England are reluctant to recognise a general right to privacy, but are willing to protect privacy interests through well-established causes of action, notably for breach of confidence, but also in appropriate circumstances by proceedings for trespass, nuisance and libel.

The High Court of Australia declined to take the opportunity given it in the *Lenah Game Meats* case to formulate a privacy right for the common law in that country.[9] In the circumstances its reluctance was not surprising. The case concerned an application by a meat processing company to keep its slaughter methods confidential; it is difficult to think of a less appropriate context in which to put a fundamental human right on a legal footing.[10] One reason for hesitation on the part of courts in both Australia and England is that existing remedies effectively protect privacy, at least in media cases. Consequently, it is unnecessary to overturn precedent denying the existence of the right. Privacy in England is also protected by the Data Protection Act 1998 and other specific regulations concerning telecommunications.[11] Complaints can be made to the Press Complaints Commission or to Ofcom (the Office of Communications). There are equivalent legal remedies in Australia.[12]

[7] [2004] 2 AC 457.

[8] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 82 (Lord Hope) and at paras. 132–3 (Baroness Hale).

[9] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199.

[10] See the judgment of Kirby J, *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at paras. 190–1.

[11] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, which implement from 11 December 2003 the requirements of the EC Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002, *OJ*, L 201, 31 July 2002, discussed below.

[12] See David Lindsay, 'Freedom of Expression, Privacy and the Media in Australia' in Madeleine Colvin (ed.), *Developing Key Privacy Rights* (Oxford: Hart, 2002) p. 157 at pp. 182–7.

Other jurisdictions have been less hesitant. Privacy rights have been given explicit statutory protection in some Canadian provinces, and in the vast majority of states in the United States. These rights have a constitutional dimension in both the United States and Canada, although in the former it is easily trumped by the First Amendment rights to freedom of speech and of the press.[13] The New Zealand Court of Appeal has now recognised a common law privacy right, where giving publicity to private or personal information would be considered highly offensive to a reasonable person.[14] Privacy rights are also protected in many civil law jurisdictions, notably in France and Germany, and are recognised by international human rights conventions, such as the International Covenant on Civil and Political Rights,[15] as well as by Article 8 of the ECHR. It therefore makes sense to refer to privacy rights or interests, even though two important common law jurisdictions still decline to recognise a discrete privacy action and prefer to protect privacy interests in other ways.

But what exactly is the right or interest at stake? The problems in defining the scope of 'privacy' are enormous. I make no attempt to resolve them in this chapter. But two related points should be emphasised. First, there is the familiar point that privacy may be infringed in a number of different ways. The most famous taxonomy of privacy invasion is that of William Prosser. In a classic article he identified four different torts: intrusion upon the claimant's seclusion, the public disclosure of true, embarrassing facts about her, publicity presenting her in a false light, and appropriation of the name or likeness (or other attribute) of a claimant for the defendant's advantage.[16] The public disclosure and false light torts almost always involve a conflict between privacy and the interests of the media, in particular their right to freedom of the press. Similar conflicts occur when the media intrude on a celebrity's personal space, for example, to take intimate photographs of her with a view to publication or besieging her home or that of her friends and neighbours, the practice known as 'door-stepping'. The intrusion tort may also be committed by the police, intelligence services, or private detective agencies, in which cases there is no conflict between privacy and freedom of speech. Moreover, intrusion by such agencies may not only invade privacy, but may, as will be explained

[13] David A. Anderson, 'The Failure of American Privacy Law' in Markesinis, *Protecting Privacy*, above n.1, p. 139.

[14] *Hosking* v. *Runting* [2005] 1 NZLR 1; see further, Gavin Phillipson in chap. 4 of this volume.

[15] Opened for signature 19 December 1966, 999 UNTS 171, 6 ILM 368 (entered into force 23 March 1976), Art. 17.

[16] William L. Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

later, inhibit the exercise of free speech rights. The fourth type of privacy infringement identified by Prosser really involves what are now known generally as 'publicity rights', where a celebrity complains that her right to market her face or voice, or some other personal attribute, has been misappropriated to her financial loss. The appropriator, say, an advertising agency, may be able to claim freedom of commercial speech. But the celebrity is not really complaining that her privacy has been infringed in these circumstances,[17] so I do not propose to say anything about this category of case.

But Prosser's taxonomy should not be regarded as exhaustive. Within the context of communications law, privacy may be infringed in ways which do not fit comfortably within his classification. For example, telephone callers and subscribers may prefer not to expose themselves to identification when making a call in order to prevent their number being used for commercial purposes. Or the recipient of a telephone call – for example a doctor whose calls are transferred from her surgery to her home at weekends – may want to keep a connected line number private. These are privacy claims, for one aspect of privacy is the freedom to choose anonymity. Another is the freedom not to be pestered by unsolicited telephone calls or emails (spams), which has been described as 'attentional privacy'.[18] That right could perhaps be accommodated within the first category of privacy invasion identified by Prosser: intrusion on the claimant's seclusion. But unlike Prosser's tort, it need not involve any invasion of her physical space, bugging or interception of her communications.

The second point about the scope of privacy rights concerns their relationship to freedom of speech and of the media. The public disclosure and false light cases do raise a *clash* or *conflict* between privacy and freedom of speech or of the press; the essence of the claim is that information about the claimant has been wrongly revealed or that false stories have been circulated about her. There is a clash between individual privacy and the public's right to know. But other types of privacy claim do not create this conflict. For example, consider two straightforward examples. An unauthorised police raid may lead to the seizure of pornographic materials. Employers may monitor the use of computers for sending obscene or hate messages. In both these circumstances, there has been an intrusion

[17] See Robert C. Post, 'Rereading Warren and Brandeis: Privacy, Property, and Appropriation' (1991) 41 *Case Western Law Review* 647.

[18] David Friedman, 'Privacy and Technology' in Ellen Paul, Fred Miller and Jeffery Paul (eds.), *The Right to Privacy* (Cambridge: Cambridge University Press, 2000) pp. 186–212 at p. 187.

on personal privacy; but in these cases, the intrusion, it can be argued, also interferes with the exercise of the right to free speech, because, in the absence of some personal privacy, individuals will be unable freely to read the material or send messages of their own choice. Further, violations of attentional privacy are remedied in order to enable subscribers to use communications systems free from the nuisance created by cold telephone calling and email and fax spams. I will discuss these particular instances in more detail in the third section of this chapter. At this juncture, it is important merely to make the point that some privacy claims support freedom of speech, rather than conflict with it.

Balancing privacy and freedom of speech in public disclosure cases

This section discusses cases where there is generally a conflict between privacy and free speech or press rights.[19] I will concentrate on the public disclosure tort, since false light cases pose relatively few difficulties. In false light cases the publication disseminates what are conceded to be untrue claims about the claimant by, for example, attributing to her remarks she never made or giving fictional (but non-defamatory) accounts of her behaviour. There is surely little public interest in their publication, particularly if they are more or less invented fabrications about aspects of the claimant's private life.[20] But restrictions on the public disclosure of true, but embarrassing information, are much more problematic, particularly when the claimant is a politician. Take the typical case of the publication by the tabloid press of the revelation that a leading politician is, or has been, having an extra-marital affair, cheats when she plays golf,[21] or is

[19] Data protection laws are not discussed in detail, although they give individuals valuable rights to regulate the processing of personal information and apply to the media as to other data controllers. The first data protection principle in the UK Data Protection Act 1998, Schedule 1, is that personal data must be processed fairly and lawfully, regard being paid to the method by which they are obtained; in a media case, one factor would be whether there has been intrusion on privacy or a breach of confidence. In *Campbell* v. *MGN Ltd* [2003] QB 633, the Court of Appeal held that a journalist is entitled to exemption under the Data Protection Act 1998, s. 32 from most of the requirements of the legislation if he reasonably believes that publication is in the public interest.

[20] See the leading decision of the German Constitutional Court in *Soraya*, 34 BVerfGE 269 (1973), where it was held that readers had no right to be informed about the former wife of the Shah of Persia through fabricated interviews.

[21] Apparently, President Clinton cheated at golf. See the references in Frederick Schauer, 'Can Public Figures have Private Lives?' in Paul et al. (eds.), *The Right to Privacy*, above n.18, pp. 293–309 at p. 300.

very ill. If she brings an action to protect her privacy, either her right to privacy, or the public's right to know and the press freedom to inform it must be sacrificed.

In this situation the law may attempt to avoid a conflict between privacy and free speech rights. Courts may deny that the latter cover the disclosure of sensitive or intimate personal information, as freedom of expression protects only serious political discussion objectively relevant to the assessment of political candidates or to someone's suitability for high judicial office. That argument is difficult to sustain as a matter of principle. If freedom of speech is prized because it allows everyone to participate in uninhibited public discourse, there is at least a presumption that people are free to discuss any attribute of an individual which the *discussants* consider to be pertinent to her holding office. A majority of people may take the view (which I share) that an individual's sexual orientation or affairs normally have nothing to do with her ability to hold public office; on this perspective, a discussion of these aspects of a politician's private life falls outside freedom of speech. But commitment to freedom of speech means that the majority cannot determine for the minority what matters are relevant to consider before voting at an election or engaging in other political activity.[22] Some people do consider it relevant to know all about someone's sexual life, or propensity to cheat at games, before casting their vote. There is no good *free speech* argument for denying that the press and other media have a right to give them that information, any more than there is for distinguishing between valuable and worthless ideas when determining which communications are entitled to free speech protection.

But equally, if privacy is to be taken seriously, it should cover a political candidate's right to keep some aspects of her most intimate personal life away from public disclosure and consequent discussion. Otherwise her right to privacy would be altogether lost. It is surely a fiction to argue that politicians and other public figures waive or surrender their privacy rights when they go into public life; there is no evidence that they do this voluntarily. Indeed, it is likely that some people choose not to enter public life, or leave it prematurely, because they do not want to run the high risk that their private lives will be torn apart by incessant media coverage. That risk weighed with Hunt J in a New South Wales libel case, when he held that it was not in the public interest to publish allegations that a former test cricketer had an extra-marital affair, since that had

[22] Ibid. pp. 297–306.

no bearing on his public life.[23] Moreover, we pay a heavy price if privacy does give way entirely to free speech in circumstances such as these. The public may incur a loss, as may the individual who decides that she cannot withstand scrutiny of her private life and must withdraw from politics. Had the same climate in which today's media compete to disclose ever more salacious details of the private lives of public figures also existed in the past, it would be hard, for example, to believe that David Lloyd George would have served as British Prime Minister in the First World War when he was carrying on an affair with his secretary, or that John Kennedy would ever have been elected as President of the United States.

The inescapable conclusion, therefore, is that both free speech and privacy rights are implicated when the press or broadcasting media reveal aspects about a politician's or celebrity's personal life. The rights must be balanced within the context of the particular facts; otherwise the courts would in effect sacrifice privacy or freedom of speech altogether in order to safeguard the other right. Balancing is a familiar process in jurisdictions where both rights are recognised, whether this is required under the constitution or is governed solely by statute and case law. In Germany, for example, the civil courts are required to assess carefully a range of relevant factors when they weigh privacy (or reputation) rights against freedom of expression.[24] Among these factors are the means used to acquire the information or take the photograph, whether the claimant had a reasonable expectation of privacy at the particular time and place, and whether the publication also involved the family and children of the politician or public figure. It is also of course relevant whether the disclosure formed part of a contribution to a discussion of politics or other matter of public concern, or amounted merely to gossip.

These principles were applied by the German Constitutional Court in its landmark ruling in the recent case involving Princess Caroline of Monaco.[25] It held the civil courts had failed to take account of the involvement of the Princess's family, when they refused to stop publication by *Bunte*, a celebrity magazine, of photographs of the Princess with her children. But the Constitutional Court rejected the argument that entertainment and celebrity stories were not covered by the free speech and press

[23] *Chappell* v. *TCN Channel 9* (1998) 14 NSWLR 153 at 172.

[24] The balancing principles were established in the early *Lüth* case, 7 BVerfGE 198 (1958), discussed in Eric Barendt, *Freedom of Speech* (2nd edn, Oxford: Oxford University Press, 2005) p. 159.

[25] 101 BVerfGE 361 (1999).

clause of the German Basic Law.[26] So the publication of photographs of the Princess shopping, riding, or tripping while at a beach club was permitted. Like the Court of Appeal in England,[27] the Constitutional Court accepted that celebrities can become role models and that there is a legitimate public interest in knowing details of their lives. A celebrity did not have a veto on the publication of photographs showing her in public, though she could stop them if they were taken while she was in a place where she had a legitimate expectation of privacy, for example, her home or the secluded part of a garden restaurant.

In a seminal ruling the European Court of Human Rights has now held that the German decisions infringed Princess Caroline's right to respect for her private life.[28] The crucial point for the court was that the tabloids had published the photos to satisfy public curiosity about a celebrity who held no public office and who did not exercise any official functions;[29] it also emphasised that the dissemination of personal photographs, in contrast to ideas, may intrude significantly into private life.[30] The German courts had attached too much weight to the position of the Princess as a prominent figure in contemporary society, and to the fact that the photographs were taken while she was in public places. In effect, the European Court held that the privacy of a public figure was infringed when her photograph was published without consent, unless it was used to illustrate a story of public importance or the person held a political or other public office.

The decisions in the Princess Caroline cases nicely illustrate how courts may come to divergent assessments of the facts when privacy is balanced against freedom of speech and the press. The assessment of the appropriate weight to be attached to each factor will also vary from one culture to another; moreover, it will change over time. Inevitably, there will be disagreements, such as that between Kirby J and Callinan J in the High Court of Australia in *Lenah Game Meats* whether it would have been right on privacy grounds not to reveal the physical impairment from which President Franklin Roosevelt suffered.[31] Probably the general view now is that it is legitimate for the media to publish details of a politician's health,

[26] Ibid. 389–91.

[27] See *A* v. *B plc* [2003] QB 195 at para. 43 (footballers are role models for young people, and undesirable conduct on their part sets a bad example. So there is a public interest in the revelation of stories about a footballer's casual extra-marital affairs).

[28] *Von Hannover* v. *Germany* (2005) 40 EHRR 1.

[29] Ibid. paras. 63–4. [30] Ibid. para. 59.

[31] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at para. 219 (Kirby J thought this restraint misconceived) and at para. 344 (Callinan J thought it right).

at least when there is reason to believe that this may affect her ability to discharge her duties; that was not the view in the US in the 1930s, nor was it in Britain in the early 1950s, when Churchill's increasing feebleness was kept hidden from the general public. Similar changes are now occurring with respect to discussion of a politician's sexual orientation or sexual conduct, though it is still not accepted, at least in England, that the media can 'out' someone as gay or lesbian without that person's consent. While, therefore, an individual's health and sexual life-style are covered by the privacy right, the scope of protection against publications concerning these aspects of personal life will vary considerably from case to case, and different jurisdictions may reach divergent conclusions.

On the other side of the scales, it is surely reasonable to question whether free speech and free press rights are entitled to the same weight against claims brought by celebrities as they are against claims by politicians in respect of similar disclosures. The English and US courts in privacy (and defamation) actions generally treat different types of speech as of equal value, irrespective whether the particular speech concerns a matter of obvious political and social importance or only reveals the escapades of footballers, pop stars, and other celebrities. Judges are understandably chary of drawing distinctions between types of speech – political or entertainment – either because they fear being considered elitist, or because it is a fundamental principle of free speech jurisprudence that all types of speech are equally valuable. There are of course dangers in drawing lines or discriminating between more and less worthy speech. But such distinctions have to be drawn, unless the privacy right is to be altogether eviscerated. It makes sense to say that free political speech is of prime importance and that, therefore, the media are entitled to report that a minister is having an extra-marital affair and so trump her privacy right. It makes much less sense to make this claim, when the claimant is a footballer or film star. Celebrities are not elected, nor do they exercise political power or claim moral leadership; the public does not have the same legitimate interest in knowing the truth about their character, as it does in knowing the truth about the private life of a member of parliament, a bishop, or perhaps a prominent businessman or newspaper editor. The European Court of Human Rights was right to reject the argument that the public is entitled to see photographs of someone like Princess Caroline, merely because they find her life interesting. The 'role model' argument, accepted by the Court of Appeal in *A* v. *B plc*,[32] is flawed. The adoption

[32] [2003] QB 195.

of, say, a footballer, film star, or Princess as a 'role model', whatever that means, does not give the public a right to know everything about these 'celebrities', so compelling them to sacrifice their privacy on the altar of idle curiosity.

Balancing between freedom of speech and privacy may be inevitable. But its disadvantages should be admitted. First, assessment of the weight of the relevant factors in particular cases is not an exact science. The results of litigation will be unpredictable; individuals anxious to protect their privacy and the media unsure whether a publication will attract a privacy action are entitled to some degree of certainty. One reason why the European Court found the approach of the German courts in the Princess Caroline case inadequate was their adoption of the conception of a 'figure of contemporary society *par excellence*' who must tolerate greater invasions of privacy than other individuals; in the European Court's view, it was too imprecise to enable someone in the position of Princess Caroline to know how to plan her life. Some legal precision can be attained by setting out the relevant factors in legislation, rather than leaving them to be determined by judges on the basis of the common law.[33]

Secondly, there is the question whether there is a presumption in favour of one right or the other: is it for a privacy claimant to show that the protection of her privacy right is so necessary that it trumps a presumption in favour of free speech, or is it for the press to show that there is a real public interest in the disclosure to outweigh what would otherwise be a plain privacy infringement? It is doubtful whether there is any short answer to this conundrum. Conceivably something might depend on how the relevant law and constitutional provisions are drafted and how the case arises. If the media in a European jurisdiction complain that a privacy law has violated their rights under Article 10 of the ECHR (the freedom of expression guarantee), the restriction imposed by the privacy rules must be justified as necessary to limit the exercise of the right to freedom of expression.[34] Equally, an individual may complain, as in the Princess Caroline litigation, that the state has failed to protect her right under Article 8 of the Convention to have her private life respected;

[33] The House of Commons Culture, Media and Sport Committee has recently recommended for this reason that it would be better to introduce a privacy right by legislation, than leave its development to the common law: UK House of Commons Culture, Media and Sport Committee, *Privacy and Media Intrusion*, Fifth Report of Session 2002–03, HC 458-I at paras. 99–111. The Data Protection Act 1998 (UK) affords a good precedent for detailed legislation in this area.

[34] ECHR, Art. 10(2).

then it would appear to be incumbent on the press to show why a limit on her privacy rights was justified in order to protect its freedom to disclose information and the right of the public to receive it. But it would not make sense to adopt a different approach according to which party was making the challenge. In the recent *Campbell* case speeches in the House of Lords indicated that neither right was entitled to priority or primacy over the other. Baroness Hale of Richmond was particularly clear on this point; in principle, the rights were of 'equal importance'.[35] The comparative weight or importance of the 'actual rights being claimed in the individual case' must be assessed, and then the justifications for, and proportionality of, the restrictions placed on them should be examined.[36] The German Constitutional Court adopts a similar approach. In contrast, the decision of the European Court in Princess Caroline perhaps indicates a preference for what is sometimes referred to in the United States as 'definitional' or 'rule balancing', under which the courts formulate a clear principle on the basis of which libel and privacy versus free speech cases are determined.[37] The rule in the Princess Caroline case is something like this: irrespective of the particular circumstances, an applicant's privacy is violated when the media publish photographs of her without her consent, unless the applicant is the holder of a public office or dissemination of the photographs is an aspect of a publication of public interest. The advantage of a rule such as this is its relative clarity and predictability, but it has the disadvantage that it may not do justice to the facts of the case.

One final point should be made briefly before we examine the types of case where privacy claims may support freedom of speech. Public disclosure (and false light) cases in practice raise a conflict between privacy and the rights of the *press* and other *media*, rather than between the former and the right of an *individual* to exercise her free speech rights. The media are of course entitled to the protection of the right to freedom of expression, largely because they provide citizens with information and provide a forum for public discussion. Courts often assume, in privacy as in other contexts, that there is no difference between free speech and free press rights; if an individual is free to tell a story, then so is the press. In the English footballer case, Lord Woolf CJ referred generally to freedom of the press and the importance of a free press. He also said that if the girls with whom the footballer had had casual affairs were free to tell their friends,

[35] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 140. [36] Ibid. para. 141.

[37] The classic example of rule balancing is the formulation by the US Supreme Court in *New York Times* v. *Sullivan*, 376 US 254 (1964) of the rule under which public officials can only succeed in a libel action, if they prove actual malice.

then they were also entitled to tell the press, with the implication that the newspapers were then entitled to exercise their press rights.[38] This argument is plausible, but certainly not incontrovertible. From the perspective of privacy, disclosure to, and by, the press is much more damaging than conversation between family and friends. Media gossip is quite different in its impact from village gossip. Further, it is not clear that the press should enjoy as wide a right to speak as do individuals. Newspapers and broadcasters are not individuals, and do not have human rights. Their potential for moral and spiritual development is not at issue if their publishing freedom is restricted, though of course their profits or even their survival might be put at risk if the restraints are particularly onerous.[39]

I do not suggest that the argument for a free press and media is not a strong one, or that it is not entitled to great weight in privacy as in other civil and criminal proceedings. But press freedom is parasitic to some extent on the underlying free speech rights and interests of readers and listeners, and the role which the press and other media play in informing them.[40] It is not the same as a free speech argument, and that should be borne in mind when we consider how much weight should be attached to the freedom when it conflicts with the right to privacy which certainly is a fundamental human right.

Privacy in support of free speech

In this part of the chapter, I consider a number of situations in which a privacy claim or right seems to support freedom of speech, rather than conflict with it. The claimant may argue that her privacy right has been infringed, with the consequence that her own freedom to communicate has been inhibited, or alternatively that the privacy claim strengthens a challenge made primarily on free speech grounds. Equally, courts may prefer to resolve a case on either free speech or on privacy grounds. For example, the European Human Rights Court treats challenges to restrictions on the freedom of prisoners to communicate by post as falling under

[38] *A* v. *B plc* [2003] QB 195 at para. 43 (iii) and (iv).

[39] Ibid. para. 11 (xii), Lord Woolf CJ suggested that courts should not ignore the fact that unless newspapers were free to publish material of interest to the public, they might not survive. This is a novel view of the public interest argument. In contrast, the European Court in the Princess Caroline case referred to the 'commercial interest of magazines' in publishing the photos: *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at [77].

[40] For a fuller statement of this argument, see Judith Lichtenberg, 'Foundations and Limits of Freedom of the Press' in Judith Lichtenberg (ed.), *Democracy and the Mass Media* (Cambridge: Cambridge University Press, 1990) p. 102.

Article 8 of the ECHR (the guarantee of the right to respect for private and family life, the home and correspondence) rather than under the Article 10 guarantee of the right to freedom of expression. But these niceties surely do not matter much. The point is that in some circumstances privacy and freedom of speech or communication go hand in hand, rather than clash with each other. I will discuss these situations under a number of headings; the list is not intended to be exhaustive and there may be some overlap between these categories of case.

Confidentiality of communications

The confidentiality of communications is certainly an aspect of the right to privacy. There is an infringement of the right whenever the security services or the police use a bugging device to eavesdrop on a conversation, tap a telephone, read email communications or monitor the use of the internet. The interference may of course be justified under a law such as the UK Regulation of Investigatory Powers Act 2000, but it is for the authorities to show that a valid warrant has been issued or other conditions for interception satisfied. But at the same time the interference also inhibits the freedom of speech of the parties to the telephone call or the email communication, although it is rare for this point to be taken. It is more likely to be made where an employer monitors employees' use of the telephone or the internet; supervision of this kind is often considered an unreasonable restraint on freedom of communication, unless there are good grounds to suspect that a particular employee has abused it.

The point arose in *Bartnicki* v. *Vopper*,[41] a recent US Supreme Court decision on the clash between privacy and freedom of the press. Vopper, a radio journalist, broadcast on his talk show a recording of an intercepted mobile telephone conversation between two union officials in which they discussed their negotiations with a local school board. Vopper had obtained the tape from the head of a local taxpayers' organisation which opposed the union's demands. It was clear that the interception and disclosure of the phone conversation violated a federal statute, the US Electronic Communications Privacy Act of 1986 (as well as analogous state laws). It amounted to a criminal offence, with civil as well as criminal penalties. The question for the court was whether application of the federal law to the broadcast violated Vopper's free speech and press rights. The majority held that it did, emphasising that the journalist had

[41] 532 US 514 (2001).

played no part in the illegal interception and that the broadcast revealed a conversation of public concern – the attitude of the union officials to the negotiations with the school board. Balancing free speech and privacy, Stevens J for the six–three majority said that privacy concerns must give way when weighed against the interest in publishing matters of public concern. But Rehnquist CJ in dissent argued that the majority decision 'diminishes, rather than enhances, the purposes of the First Amendment: chilling the speech of the millions of Americans who rely upon electronic technology to communicate each day'.[42] The federal statute was not only concerned to protect privacy, but to further the free speech rights of the parties to telephone conversations. Moreover, the union negotiators did not intend to contribute to public debate, but were engaged, so far as they were concerned, in a purely private conversation, albeit about a matter of public concern.

This case is important, because it shows that it is too simple to treat breach of confidence cases as necessarily raising a straight conflict between free speech on the one hand, and privacy (or confidentiality) on the other. The issues may well be more complex than that. To allow the media to publish an intercepted conversation, or other material such as a personal diary, might lead overall to a loss of free speech. Of course, that loss is conjectural, while the interference with Vopper's First Amendment rights would have been real, had the case been decided the other way. Nonetheless, it is surely legitimate to take into account in assessing the strength of a privacy (or confidentiality) claim that any infringement of that right may also damage the exercise of individuals' free speech rights.

Similar issues arise in a different context. Journalists claim that they are entitled to a privilege to keep the identity of their sources confidential, in order to encourage the sources to speak freely and so enable the press to report stories of real public interest.[43] The privilege protects the anonymity or privacy of the source, and also her freedom to talk openly to the press, and its freedom to pass on the story to the general public. Privacy and freedom of expression go hand in hand, as they do when an action for breach of confidence is brought to restrain private conversations between, say, spouses or partners. On the other hand, there may be a conflict between the privacy and free speech rights of the source on the

[42] *Bartnicki* v. *Vopper*, 532 US 514 at 554 (2001).

[43] The privilege is recognised by English law in s. 10 of the Contempt of Court Act 1981. It is also recognised by the European Court of Human Rights as an integral aspect of the freedom of expression: *Goodwin* v. *UK* (1996) 22 EHRR 123.

one hand and freedom of the press on the other. This is brought out by the case of *Cohen* v. *Cowles Media Co.*[44] A newspaper decided to break its promise of confidentiality to a source, because the editor considered that disclosing the identity of the source, a consultant employed by the Republicans, would strengthen the story he had given the paper about the shop-lifting conviction of the Democrat candidate for state Lieutenant Governor. The US Supreme Court held that the press did not have a First Amendment immunity to the source's action for breach of the confidentiality promise. The source's right to talk to the press on conditions of anonymity was not trumped by its own First Amendment rights.

Possession of pornographic material

A second group of cases where privacy and free speech rights seem to go hand in hand concern the right to possess and read pornography, particularly at home, where it is clear that the possessor does not intend to publish the material or distribute it to children. Two cases illustrate this position. In *Stanley* v. *Georgia*[45] the US Supreme Court reversed a conviction for possessing obscene matter, three reels of pornographic film found in the defendant's home. Marshall J based the court's opinion on both the fundamental First Amendment right to receive information and ideas and the right to be free from unwarranted intrusions on privacy. The two were merged, when he emphasised that the defendant was claiming the right to read or view what he pleased in the privacy of his own home. More recently, the Supreme Court of Canada has examined the compatibility of the offence of mere possession of child pornography (without intent to distribute the material) with the Charter right to freedom of expression.[46] The constitutionality of the offence was also challenged on the ground that it violated the right to liberty, guaranteed by section 7 of the Charter, in which privacy is implied. McLachlin J for the court did not think the latter argument required separate consideration from that given the freedom of expression challenge. However, in her view the privacy claim enhanced the freedom of expression argument. Material held privately occasioned less harm than published material, and privacy in this context was closely linked to the freedom of conscience and belief which underlie freedom of expression.[47]

[44] 501 US 663 (1991). [45] 394 US 557 (1969).
[46] *R* v. *Sharpe* [2001] 1 SCR 45. [47] Ibid. 72.

Prisoners' correspondence

As already mentioned, claims by prisoners that the interception or stopping of their correspondence or telephone calls to legal advisers, relatives, and friends violate their Convention rights are almost always considered under Article 8 of the ECHR rather than under Article 10 guaranteeing freedom of expression.[48] It would be wrong to infer that freedom of expression is not implicated; it is rather that, in the European Human Rights Court's view, Article 8 with its explicit mention of the right to respect for correspondence is the *lex specialis,* to which primary consideration should be given. There is no need to consider other provisions of the Convention. If, however, a prisoner complains that he has been denied the right to read newspapers or to watch television, the case will be considered under Article 10.[49] (In a number of cases, the court has held that any claim to an access right to information under the Convention should be based on Article 8, rather than on Article 10;[50] in this context, the scope of freedom of information is cut down by its linkage to the right to respect for private and family life, so that there are only access rights to get hold of personal, rather than general policy, information.)

Anonymity and restriction on caller and connected line identification

In many circumstances a right to anonymity may be provided by statute, or asserted at common law, in order to protect personal privacy. Many of these circumstances arise in the context of litigation, of which perhaps the best known examples are the anonymity accorded complainants of rape and other sexual offences (though not adults accused of these or of other offences) and children involved in legal proceedings, either as defendant or as a witness. In these circumstances, privacy or anonymity conflicts with the freedom of the media to report full details of legal proceedings.

In other circumstances, however, a right to anonymity may be upheld as necessary to allow freedom of individual speech and communication. Bans on the distribution of anonymous handbills and election campaign literature have been held unconstitutional in the US for infringing freedom of speech;[51] these bans also infringe privacy. Equally, a right on the

[48] *Silver* v. *UK* (1983) 5 EHRR 347; *McCallum* v. *UK* (1991) 13 EHRR 597.
[49] See *Herczegfalvy* v. *Austria* (1992) 15 EHRR 437.
[50] *Leander* v. *Sweden* (1987) 9 EHRR 433; *Gaskin* v. *UK* (1988) 12 EHRR 36.
[51] *Talley* v. *California*, 362 US 60 (1960); *McIntyre* v. *Ohio Election Commission*, 514 US 334 (1995).

part of adults to waive anonymity may also be upheld as an aspect of both privacy or personality rights on the one hand and free speech on the other. That is shown in a German case, where the Constitutional Court ruled that the complainant, a woman of 41, was entitled to use her own name and, therefore, by implication to name her father, when she made public allegations that he had sexually abused her as a child.[52] The court held that the order of the state appeal court requiring her not to make these allegations using his name or in her own name infringed her right to freedom of expression. To use her own name would give greater authenticity to her statements, and encourage other women to come forward. But equally, a restriction on the use of one's own name infringed an attribute of one's identity and personality. There was an infringement of both Article 2 (the right to free development of the personality) and Article 5 (right to freedom of expression) of the Basic Law.

The phenomenon of Caller ID (Caller Identification) for telephone, and now email communications, provides an important context for consideration of anonymity and freedom of speech.[53] Caller ID provides benefits for any called person who is able by this means to trace nuisance callers, but it is particularly valuable for delivery services who can ignore hoax customers, and of course for telemarketers who can build up lists of customers. On the other hand, it may inhibit the privacy and the exercise of free speech of some callers, say, police informants, battered women, and others using help-lines and support services. A European Union Directive on the protection of privacy in the electronic communication sector takes account of the interests of callers who wish to protect their anonymity and those of the recipients of telephone communications who may want to reject incoming calls when the caller has prevented Caller ID.[54] A caller must be given the possibility free of charge to prevent identification on a per call basis, while a subscriber must have the opportunity to do this for all calls on her line. Caller anonymity may be overridden when a subscriber wants to trace malicious or nuisance calls, or to enable emergency services such as the ambulance and fire services to respond to calls.[55] Subscribers have a similar right not to be listed in telephone directories,

[52] 97 BVerfGE 391 (1998).

[53] For a short discussion of this topic in an American context, see Judith Wagner DeCew, *In Pursuit of Privacy* (Ithaca, New York: Cornell University Press, 1997) pp. 153–62.

[54] Directive 2002/58/EC of 12 July 2002, above n. 11, Art. 8. It replaces an earlier Directive of 1997 which was confined in scope to telecommunications. (For implementation of these provisions in UK law, see SI 2003/1246, regs. 10–19.)

[55] Ibid. Art. 10.

or to withhold personal data, such as their sex or details of their address.[56] The rules requiring communications systems to allow callers to prevent Caller ID are surely sensible privacy protection rules. They can also be defended in terms of encouraging use of the system and so promoting the exercise of free speech, for some people would undoubtedly be deterred from making calls if their identity were revealed to the recipient. Telecoms companies, and business interests in the United States, have resisted the introduction of these rules, but not, it seems, on the ground of any free speech or other constitutional principle.[57]

Protection against spams and cold calling

The EU Directive, and UK regulations implementing it,[58] also protect users of communications systems against spams and cold calling. The use of automated calling machines, fax machines or email for direct marketing may only be allowed in respect of subscribers who have given their prior consent, though for cold telephone calling member states have the choice whether to require subscribers to opt in or enable them to opt out – in either case free of charge.[59] (The United Kingdom has chosen an opt-out arrangement.)[60] These regulations protect the attentional privacy of telephone and email users, although arguably they restrict the freedom of cold callers and the senders of spams to engage in commercial speech.

The issue has arisen in litigation in the United States. Following protests from their subscribers, America On Line (AOL) and Compuserve took steps to stop Cyber Promotions sending unsolicited email messages (spams), unless the subscriber ticked a Box labelled, 'I want junk email'. In two cases, federal district courts have rejected the argument that Cyber Promotions had a First Amendment right to send spams to AOL and Compuserve subscribers.[61] The argument turned on familiar principles of US free speech jurisprudence. Mail servers are not a public forum for speech,

[56] Ibid. Art. 12. Rights not to be included in a directory, or to check and correct personal data are to be free of charge.

[57] See DeCew, *In Pursuit of Privacy*, above n. 53, pp. 157–8.

[58] SI 2003/2426, regs. 19–24.

[59] Directive 2002/58/EC of 12 July 2002, above n. 11, Art. 13. There is a limited exception to the opt-in requirement for automated calling machines etc., where a supplier obtains from a customer her electronic contact details in the context of a sale. He can use these details for direct marketing 'of its own similar products or services', though the customer has a right to object to the use of these details.

[60] SI 2003/2426, reg. 21.

[61] *Cyber Promotions* v. *AOL*, 948 F Supp 436 (ED Pa., 1996); *Compuserve Inc* v. *Cyber Promotions*, 962 F Supp 1015 (SD Ohio, 1997).

to be equated with streets and public parks. Internet service providers are private actors, so they are fully entitled to determine who has access to their communication systems. They are entitled to protect their own property rights against the access claims of the email spammers. The real beneficiaries of the litigation were the users of the electronic mail systems who had pressured AOL and Compuserve to act. Moreover, in both cases the court took the point that the viability of these communications systems might be put in danger if the claims of the spammers were upheld. Limiting the spammers' freedom would in the long term encourage use of electronic communications for the exercise of free speech. In other words, this is another situation where the privacy interests of the subscribers go hand in hand with the overall promotion of free speech. Adopting similar principles, a Circuit Court of Appeals has recently rejected a First Amendment challenge brought by telemarketers to federal rules proscribing cold commercial calls to telephone subscribers who had registered that they did not wish to receive such calls.[62] The privacy and, it may be argued, the free speech interests of telephone subscribers were given more weight than the commercial free speech rights of the telemarketers.

Conclusion

Privacy and freedom of speech do not always clash. Indeed, there are many circumstances in which a claimant may assert both rights. This should not be a matter of surprise. We have become accustomed to thinking that these rights *inevitably* conflict. But we take this view, only because that is what happens in the typical context in which we consider their relationship: a claim by a public figure that her privacy has been infringed by press reporting of some scandal or gossip. In an age when communication has been dominated by the press and broadcasting media, we have lost sight of the free speech interests and rights of individuals, or at least paid them less attention. The cases of conflict, as I have said, almost invariably involve a clash between individual privacy and press or media freedom.

However, when we look at free speech as the right of individuals to express their ideas and to share views and information with others, then we should adopt a different perspective. One value of privacy, and a reason why it is recognised as a constitutional or legal right, is that it gives individuals the space to develop their own identity by themselves, and

[62] *Mainstream Marketing* v. *Federal Trade Commission*, 358 F 3d 1233 (10th Cir. 2004). On 5 October 2004, the Supreme Court declined to consider the case.

in communication and cooperation with friends and lovers, free from observation and interference by Big Brother or even by a liberal democratic state.[63] Some privacy is essential to enable us to read, contemplate and formulate thoughts, and some confidentiality and security is similarly necessary to exchange ideas with friends and colleagues. That at any rate was the experience in the eighteenth century, when property rights – we would now identify the rights as personal privacy interests – were used to safeguard radicals against the arbitrary confiscation of their manuscripts and papers.[64] It is also important to note that privacy has a social dimension. It is not concerned only to protect individuals acting entirely in isolation from each other; rather, '[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.'[65]

The internet and email communications make it possible for individuals to communicate their ideas with each other without geographical limit, and without use of the mass media. That is why this development is potentially, some would say already, the most important media development since the advent of the printing press. Whether in the context of political speech, electronic communications will supplant, or only supplement, the traditional newspaper and broadcasting media has yet to be determined. But they will without doubt play an increasingly substantial role in spreading new political causes and enabling groups to organise and expand. In this context we should re-evaluate the relationship of personal privacy and freedom of speech. While privacy rights and the interests of the mass media may often conflict, the same is not always true of privacy and the speech rights of individuals. Instead, some privacy protection is necessary for them to exercise their speech rights free from anxiety and inhibition.

[63] For essays emphasising this aspect of privacy, see in particular James Rachels, 'Why Privacy is Important' (1975) 4 *Philosophy and Public Affairs* 323 and Jeffrey H. Reiman, 'Privacy, Intimacy, and Personhood' (1976) 6 *Philosophy and Public Affairs* 26.

[64] *Wilkes* v. *Wood* (1763) 19 State Trials 1193; *Entick* v. *Carrington* (1765) 19 State Trials 1030.

[65] The European Court of Human Rights in *Niemietz* v. *Germany* (1993) 16 EHRR 97 at para. 29.

3

Revisiting the American action for public disclosure of private facts

BRIAN C. MURCHISON

The 1981 American film *Absence of Malice*, although lopsided against the press in its account of journalism gone bad, contains one indelible scene. In a Miami neighbourhood's early morning hours, a tense young woman sits on a front porch, waiting for the newspaper boy. Soon enough, he pedals up the street and tosses papers on all the identical yards, finally reaching hers. She anxiously pulls the paper from its plastic bag and clumsily unfolds it. The story is on page one. We don't see what it says, but we know. It reports that she, a Catholic secretary in a parochial school, had an abortion the previous year, and that on the day of the abortion, she was accompanied by a man who is suspected of killing a union leader on the same day. Her story is news; she could be the suspect's alibi. She slowly refolds the paper and forces it back in its container. She then runs in despair to all the other yards, gathering each paper: her world must not learn about the abortion. Of course, her efforts are futile.

The irony of the scene is compelling. Although American constitutional law strongly protects individuals from the state's usurpation of highly intimate decisions – relating to such things as contraception, abortion, and sexual conduct[1] – the common law is famously tentative in shielding individuals from privacy invasions by the press, even about the same matters.[2] To be sure, the *Restatement (Second) of Torts* provides that when

I wish to thank Dean David Partlett and Professors Blake Morant and Megan Richardson for their helpful comments; Christopher Vrettos for invaluable research assistance; and the Frances Lewis Law Center for supporting the project.

[1] For a review of the contraception and abortion cases, see Ellen Alderman and Caroline Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995) pp. 55–66. At the end of its 2003 term, the Supreme Court struck down on due process grounds a state law criminalising homosexual sodomy, *Lawrence* v. *Texas*, 539 US 558 (2003).

[2] See generally Diane L. Zimmerman, 'Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort' (1983) 68 *Cornell Law Review* 291.

one party publicises private facts about another, and disclosure would be highly offensive to a reasonable person and is unrelated to a matter of legitimate public concern, the subject of the disclosure has a cause of action for damages.[3] However, in such suits for 'public disclosure of private facts', plaintiffs often fail to establish that the disclosure lacked relevance to a matter of 'public concern'.[4] If the young woman in *Absence of Malice* had sued for public disclosure, she likely would have lost, perhaps not even reaching a jury.[5]

Consider a recent example. In *Shulman* v. *Group W Productions Inc.*,[6] a car ran off a highway and overturned. The plaintiffs, a mother and son, were trapped inside. A rescue team arrived, including a nurse who wore a wireless microphone provided by a television producer. The producer's cameraman was also at the site. Unknown to the victims, the nurse and cameraman recorded their condition after the crash, their removal from the car, the mother's expressions of 'disorientation and despair',[7] and her agony inside a rescue helicopter. Months later, a television station aired a programme on emergency medicine, including footage obtained that night, and the mother watched in disbelief from her hospital bed. In her action for public disclosure of private facts, she protested the 'gruesome' footage and testified that 'it's not for the public to see this trauma that I was going through'.[8] The television station defended on the ground that footage of the mother's appearance and speech during the rescue operation were 'substantially relevant' to a matter of public concern.[9] The California Supreme Court agreed, finding a public matter in the accident itself and 'the rescue and medical treatment of accident victims'.

[3] *Restatement (Second) of Torts* (St Paul, Minn.: American Law Institute, 1977) s. 625D. Building on a classic article, Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, William Prosser identified 'a complex of four' causes of action relating to invasion of privacy, see W. Page Keeton (ed.), *Prosser and Keeton on Torts* (5th edn, St Paul, Minn.: West, 1984) p. 851. The public disclosure tort has been called the 'quintessential cause of action for invasion of privacy': Rodney A. Smolla, 'Accounting for the Slow Growth of American Privacy Law' (2002) 27 *Nova Law Review* 289 at 296.

[4] Robert D. Sack, *Sack on Defamation: Libel, Slander, and Related Problems* (3rd edn, New York: Practising Law Institute, 1999), paras. 12–42 and 12–54 (noting difficulty of establishing lack of 'newsworthiness').

[5] The character's situation in the film is complicated by the fact that she herself gave the information about the abortion to a reporter, albeit without grasping that she was (in the reporter's words) 'talking to a newspaper' and therefore speaking 'on the record'. However, even if the reporter independently had discovered the private fact, a suit for 'public disclosure' would fail if a reasonable editor could conclude that the fact was substantially relevant to a newsworthy topic: *Gilbert* v. *Medical Economics Co.*, 665 F 2d 305 at 309 (10th Cir. 1981).

[6] 955 P 2d 469 (Cal. 1998). [7] Ibid. 488. [8] Ibid. 476. [9] Ibid. 488.

Because the specific footage of the mother showed the challenge faced by emergency workers, it was 'substantially relevant' to the general topic and had 'legitimate descriptive and narrative impact'.[10]

The plaintiffs in *Shulman* join a long list of others who have lost public disclosure claims: a one-time child prodigy, famous in youth but reclusive as an adult, whose odyssey became the subject of a 'merciless . . . dissection' by James Thurber in the *New Yorker* magazine;[11] a man who deflected an attempt on the life of an American President in 1975, and then became the subject of unwanted news accounts identifying him as homosexual;[12] a young adult who was sterilised against her will in a county home for troubled youths and then found her sterilisation reported in a newspaper's account of the home's practices;[13] a rape-murder victim's father, who sued after a television station found the victim's name in court papers and broadcast it over the air;[14] a rape victim whose family received anonymous threatening phone calls, possibly from her attacker, after a newspaper published her name;[15] an adoptive mother and her daughter, who sued a newspaper for printing details of the child's history and the conflict caused by the birth mother's sudden reappearance.[16] In each case, courts held that the disclosures were privileged.

Plaintiffs who fared better in the courts included a college student body president who sued a newspaper for disclosing that she was a transsexual,[17] a mother who sued a newspaper for publishing words she spoke over her dead son's body in a private hospital room,[18] and a celebrity couple who challenged the internet distribution of a videotape depicting their sexual activities.[19]

[10] Ibid. 488–9.

[11] *Sidis* v. *F-R Publishing Corporation*, 113 F 2d 806 at 807 (2nd Cir.), cert. denied, 311 US 711 (1940). See *Rosenbloom* v. *Metromedia Inc.*, 403 US 29 at 80 (1971) (Marshall J dissenting, noting that although the former prodigy 'had a passion for obscurity', disclosure of his 'somewhat peculiar behavior . . . was found to involve a matter of public concern').

[12] *Sipple* v. *Chronicle Publishing Co.*, 201 Cal. Rptr 665 (1984).

[13] *Howard* v. *Des Moines Register & Tribune Co.*, 283 NW 2d 289 (Iowa 1979).

[14] *Cox Broadcasting Corp.* v. *Cohn*, 420 US 469 (1975).

[15] *The Florida Star* v. *BJF*, 491 US 524 (1989).

[16] *Hall* v. *Post*, 372 SE 2d 711 (NC 1988).

[17] *Diaz* v. *Oakland Tribune Inc.*, 188 Cal. Rptr 762 (App. 1983) (rejecting press argument that student leader's gender was newsworthy as a matter of law).

[18] *Green* v. *Chicago Tribune Co.*, 675 NE 2d 249 at 256 (App. Ct Ill. 1996) (holding that a jury could find that the public 'has no concern with the statements a grieving mother makes to her dead son').

[19] *Michaels* v. *Internet Entertainment Group Inc.*, 5 F Supp. 2d 823 at 842 (CD Cal. 1998) (holding that plaintiffs demonstrated a likelihood of success in meeting the burden of showing that contents of tape were not newsworthy). In a related case, the court held that

Although some commentators have proclaimed the death of the public disclosure tort,[20] the action has stubbornly survived, as if determined to outlast the courts' apparent confusion about the interest at stake and the proper means of addressing that interest without subverting hallowed rights of expression.[21] This chapter's thesis is that the public disclosure tort cannot be understood apart from the Supreme Court's development of another tort – the common-law action for libel – in the years just before the court's first public disclosure case. At the heart of libel jurisprudence was a concern for the dignity of citizens and publishers in speaking out on public issues. Protecting the value of equal democratic participation, the court energetically developed an elaborate matrix of libel doctrine. However, as the privacy tort came before the court in the mid-1970s, its own core proved comparatively elusive, and the court lacked theoretical fuel for doctrinal development. After comparing the court's extensive cultivation of one doctrinal field with its spare treatment of another, the chapter proposes a basis for a revitalised, if still narrow, public disclosure tort, drawing in particular on the court's recent decision in *Bartnicki v. Vopper*,[22] and the insights of several contemporary thinkers on the indispensable role of privacy in the development of self.

What's wrong with the public disclosure tort?

Commentators offer various explanations of the public disclosure tort's doctrinal thinness and uncertain reach. One account cites American culture's pervasive acquiescence in privacy invasion. A second emphasises the

a tabloid television programme's story on the videotape, including brief excerpts from the tape itself, was newsworthy as a matter of law: *Michaels* v. *Internet Entertainment Group Inc.*, 27 Med L Rep 1097 at 1104–5 (CD Cal. 1998).

[20] E.g., Zimmerman, 'Requiem for a Heavyweight', above n. 2, 365 (arguing that the public disclosure tort addresses a problem 'incapable of resolution in the courts' and therefore should be given 'a well-deserved rest'). However, the opinions of five justices in *Bartnicki* v. *Vopper*, 532 US 514 (2001), appear to 'endorse the principal ingredients' of the public disclosure tort: Rodney A. Smolla, 'Information as Contraband: The First Amendment and Liability for Trafficking in Speech' (2002) 96 *Northwestern University Law Review* 1099 at 1150.

[21] *New York Times* columnist Anthony Lewis suggests that 'it is not inconsistent with the great function of the press in keeping power accountable to have some concern for the feelings of those who have not sought power, for [the ex-prodigy profiled in the *New Yorker*] or [the crash victim recorded by the rescue nurse], for example': Anthony Lewis, 'Privacy and Civilization' (2002) 27 *Nova Law Review* 225 at 238. Lewis concludes that the privacy of private individuals 'is an essential component of a civilized life', at 242.

[22] 532 US 514 (2001).

reluctance of the narrower United States legal culture to accept responsibility for fashioning doctrine for the protection of privacy. A third explanation underscores the supposedly elusive nature of the privacy interest itself.

An example of the first account is David A. Anderson's suggestion that American citizens are two-faced about privacy: they claim to respect it 'but in fact [they] devour the private secrets of hundreds of people everyday'.[23] Anderson concedes that the culture values privacy, but he maintains that Americans simultaneously 'hunger to know – to know the shocking details of scandal, to see the drama of terror or grief or humiliation, to understand the strangeness of our neighbors. The law merely reflects our ambivalence.'[24] He notes that journalism schools stress that 'news is about people', and that the media's inclination to personify both breaking news and long-term social analysis is accepted by a populace whose 'curiosity' about private facts is insatiable.[25] Rodney A. Smolla similarly traces the weakness of legal privacy to Americans' penchant for gossip.[26] Given the culture's disregard of privacy, Smolla is unsurprised that invasion of privacy has small stature in tort law.

These arguments from sociology are intriguing but not altogether persuasive. American 'hunger' for details of scandal and public drama does not necessarily indicate approval of, or even ambivalence about, the sorts of revelations that prompt most public disclosure suits. Those revelations usually appear in local news or feature stories about individuals who have not consented to coverage and whose circumstances strongly suggest that media exposure will cause them harm. It is not at all self-evident that the curiosity of even American television audiences extends to the hidden plights of involuntary news figures such as car crash survivors, adoptive children, or rape victims. As for the argument that a culture of gossip signals a general disrespect for privacy, it is worth noting that everyday gossip is a far cry from the 'publicity' addressed by the public disclosure tort.[27] Moreover, since the impact of gossip is usually quite different from that of media publicity, participation in gossip is at best slim evidence of acquiescence in media dissemination of private facts. Gossipers chatter with others about a third party; the insult to the third party is usually

[23] David A. Anderson, 'The Failure of American Privacy Law' in Basil S. Markesinis (ed.), *Protecting Privacy* (Oxford: Oxford University Press, 1999) p. 141.

[24] Ibid. [25] Ibid. p. 142. [26] Smolla, 'American Privacy Law', above n. 3, 305.

[27] See *Restatement (Second) of Torts* s. 652D (distinguishing speech to 'a single person or even . . . a small group of persons' from 'publicity' required by the tort, and defining publicity as that which makes a matter 'public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge').

indirect.[28] In contrast, when a news outlet transmits a person's intimate facts to the public, the audience may well include the person in question. As the plaintiff in *Shulman* surely discovered as she watched her own suffering on television, the impact of a media outlet's invasion of privacy is direct. For these reasons, it is difficult to attribute the weakness of the privacy tort to widespread cultural acceptance of, or participation in, similarly invasive behaviour or speech.

Another explanation for the weakness of the tort relates to the country's *legal* culture. Anderson posits that judges are 'extremely reluctant to decide what is private' because they think that society is too diverse to produce common norms of privacy. He adds that judges are 'unwilling to decide what matters are of legitimate public concern' because they have no desire to second-guess editors and risk violating liberties of speech and press.[29] Similarly, Smolla cites the legal culture's 'ingrained skepticism' about penalising truthful publications, even if the published facts were private, and the judiciary's reluctance to overrule editorial choices.[30]

This account has more power than the first but still falls short. If the legal culture is reluctant to impose damages on accurate yet invasive publications, it has had the opportunity to declare a categorical privilege for truthful publications since at least 1975.[31] However, the Supreme Court has deliberately declined to take that course, and only a handful of states have rejected the public disclosure tort.[32] As for the intractability of issues relating to 'matters of public concern', such issues arise in libel cases fairly frequently without inhibiting judges. Similar questions concerning whether a plaintiff has voluntarily injected him or herself into a 'public controversy' are not considered beyond judicial capacity.[33] In deference

[28] See Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Pantheon, 1982) p. 91 (defining gossip as 'informal personal communication about other people who are absent or treated as absent').

[29] Anderson, 'The Failure of American Privacy Law', above n. 23, 148–51.

[30] Smolla, 'American Privacy Law', above n. 3, 304.

[31] See *Cox Broadcasting Corp.* v. *Cohn*, 420 US 469 at 491 (1975) (recounting press argument for broad holding on truthful publications).

[32] Jonathan B. Mintz, 'The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain' (1996) 55 *Maryland Law Review* 425 at 432–3 n. 37 (citing West Virginia, New York, Minnesota, Nebraska, and North Carolina as jurisdictions that do not recognise the tort).

[33] See, e.g., *Dun & Bradstreet Inc.* v. *Greenmoss Builders Inc.*, 472 US 749 at 761–3 (1985) (discussing whether a credit report involved a 'matter of public concern'); *Waldbaum* v. *Fairchild Publications Inc.*, 627 F 2d 1287 at 1296 (DC Cir. 1980) (discussing whether a libel plaintiff had injected himself into a pre-existing 'public controversy', thereby meeting one of the requirements of a limited-purpose public figure); *Lohrenz* v. *Donnelly*, 350 F 3d 1272 (DC Cir. 2003) (finding that female combat pilot is a limited-purpose public figure).

to the First Amendment, judges may choose to favour speech interests in privacy cases,[34] but their readiness to decide a variety of similar issues in libel suits shows that legal resources are not lacking for the field of privacy.[35]

A third, more convincing analysis is that the privacy tort falters because the Supreme Court has failed to articulate a clear concept of privacy in this context, leaving lower courts in considerable doubt about the value of vigilant protection.[36] Courts clearly exhibit surer grasp of the countervailing interest – democratic society's dependence on open communication on public matters, even intimate matters touching on public issues – than of a plaintiff's need to withhold private facts from the public eye. Judicial pronouncements on privacy in the media context range from the unhelpfully broad, such as Justice Potter Stewart's declaration that 'the protection of private personality' is 'a basic of our constitutional system',[37] to the impossibly narrow, such as Judge Richard Posner's emphasis on the privacy of basic bodily functions.[38] Within these extremes, a few courts have been willing to intimate that privacy's basis is negative liberty,[39] or positive liberty,[40] but none has voiced anything resembling Justice Anthony Kennedy's account of the components of self-determination in the constitutional cases.[41]

[34] See, e.g., *Hall* v. *Post*, 372 SE 2d 711 at 721 (NC 1988) (Frye J concurring) (noting that 'the legitimate concerns to the public must be defined in the most liberal and far-reaching terms in order to avoid any chilling effect on the constitutional right of the media to publish information on public interest').

[35] See Smolla, 'American Privacy Law', above n. 3, 300 (arguing that 'basic legal standards which have evolved' with respect to the category of 'public controversy' in libel law 'are coherent and functional').

[36] For an interesting survey of the multiple interpretations of privacy in American legal thought, see Jonathan Kahn, 'Privacy as a Legal Principle of Identity Maintenance' (2003) 33 *Seton Hall Law Review* 371.

[37] *Rosenblatt* v. *Baer*, 383 US 75 at 92 (1966) (Stewart J concurring).

[38] *Haynes* v. *Alfred A. Knopf, Inc.*, 8 F 3d 1222 at 1229 (7th Cir. 1993).

[39] E.g., *Hall* v. *Post*, 355 SE 2d 819 at 824–6 (NC App. 1987) (characterising plaintiff's interest as the 'right to have others not know', and 'the individual's right to be free from unwarranted exposure'), reversed on other grounds, 372 SE 2d 711 (NC 1988) (declining to recognise public disclosure tort in North Carolina).

[40] E.g., *Beaumont* v. *Brown*, 257 NW 2d 522 at 527 (Mich. 1977) (noting that '[i]n this ever advancing society all are concerned that the individual's integrity and independence are not obliterated by the dissemination of unnecessary information about his private life').

[41] E.g., *Lawrence* v. *Texas*, 539 US 558 at 562 (2003) (stating that '[l]iberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct', and that respect for 'the dignity of free persons' counsels against state attempts 'to define the meaning of [a voluntary personal] relationship or to set its boundaries absent injury to a person or abuse of an institution the law protects'). *Lawrence* also cited a famous

Perhaps the courts cannot be faulted for failing to develop a strong concept of privacy in the media context; after all, leading public disclosure cases have presented a dizzying diversity of claims, obscuring any common feature that could facilitate grasp of a core interest. For some plaintiffs, privacy seems to be a means of isolating seriously limiting past events in order to surmount their emotional effects and set one's own terms for current relationships.[42] In such cases, the privacy interest as a concept of self-realisation arguably assumes its most compelling form. Less persuasively, other plaintiffs invoke privacy as a means of barring mention of a traumatic present event, as if to maintain that, on some level, the event did not actually happen.[43] Here, privacy is a form of denial, with nothing obvious to commend it. In other cases, privacy is a means of resisting the market, a vehicle for withholding consent from the media's use of intimate facts to garner ratings and advertising dollars.[44] This sort of claim is less about self-realisation or emotional distress than it is about checks and balances, the felt need to resist exploitation. Privacy can also function as a security interest against possible physical harm resulting from mass disclosure of identity.[45] If the shadings of privacy are indeed this various, courts may be reluctant to enforce an interest whose meanings shift, with some less strong than others.

A number of scholars, however, argue that the meaning of privacy is not ambiguous. They maintain that at privacy's core is a clear interest in dignity. Thus, forty years ago, Edward Bloustein posited that a concern for 'the individual's independence, dignity, and integrity' was the basis of each of the torts of invasion of privacy.[46] More recently Jonathan Kahn has suggested that privacy and dignity are related in a specific way: privacy lays the groundwork for dignity by creating conditions of 'individuation'.[47] For

passage from *Planned Parenthood of Southeastern Pa.* v. *Casey*, 505 US 833 at 851 (1992): 'At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under the compulsion of the State.'

[42] E.g., *Sidis* v. *F-R Publishing Corp.*, 113 F 2d 806 at 807 (2nd Cir.), cert. denied, 311 US 711 (1940). See below nn. 127–9 and accompanying text.

[43] E.g., *Cox Broadcasting Corp.* v. *Cohn*, 420 US 469 (1975). See below nn. 70–2 and accompanying text.

[44] E.g., *Shulman v. Group W Productions Inc.*, 955 P 2d 469 (Cal. 1998). See above nn. 6–10 and accompanying text.

[45] E.g., *The Florida Star* v. *BJF*, 491 US 524 (1989). See below nn. 73–80 and accompanying text.

[46] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962 at 971.

[47] Kahn, 'Privacy as a Legal Principle', above n. 36, 378.

Kahn, 'invasions of privacy . . . affront dignity insofar as they undermine the integrity of one's identity'.[48] But how does individuation occur, and why have American courts been deaf to arguments relating common law privacy to dignity? This chapter next suggests that, wisely or not, the Supreme Court's libel jurisprudence effectively pre-empted the concept of dignity, treating it as a value of political participation relevant to the dynamics of libel disputes but less clearly applicable to cases involving non-public dimensions of life. As a result, the public disclosure tort has been in search of its own animating basis, a project that is still underway.

Dignity and the libel tort

In 1964, the Supreme Court issued its decision in *New York Times Co.* v. *Sullivan*,[49] contemporaneously hailed as 'the best and most important [opinion] ever produced in the realm of freedom of speech'.[50] In an action for libel brought by a state police commissioner against civil rights workers and the *Times*, the Supreme Court held that the libel tort could not be squared with the dictates of the speech and press clauses of the First Amendment. Writing for the court, Justice Brennan likened the libel tort to the infamous Sedition Act of 1798, and declared that the 'central meaning of the First Amendment' was that 'the censorial power is in the people over the Government, and not in the Government over the people'.[51] The court thus ruled that, in addition to the tort's common law elements, a public official who sues a 'citizen critic'[52] of his or her official conduct must prove clearly and convincingly that the contested statement was false and that the speaker either knew it was false or had serious doubts about its truth.[53]

[48] Ibid. [49] 376 US 254 (1964).

[50] Harry Kalven Jr, 'The New York Times Case: A Note on "The Central Meaning of the First Amendment"' [1964] *Supreme Court Review* 191 at 194. First Amendment lawyer Floyd Abrams has called Sullivan a 'majestic decision', quoted in Anthony Lewis, *Make No Law: The Sullivan Case and the First Amendment* (New York: Random House, 1991) p. 156.

[51] 376 US 254 at 275, 282 (1964). Justice Brennan's opinion exemplified what Benjamin Cardozo decades earlier had called the 'chief worth' of the 'restraining power of the judiciary': 'making vocal and audible the ideals that might otherwise be silenced, in giving them continuity of life and of expression, in guiding and directing choice within the limits where choice ranges': Benjamin N. Cardozo, *The Nature of the Judicial Process* (New Haven: Yale University Press, 1921) p. 94. Cardozo was a defender of judicial review 'exercised with insight into social values, and with suppleness of adaptation to changing social needs'.

[52] *New York Times Co.* v. *Sullivan*, 376 US 254 at 282 (1964).

[53] Ibid. pp. 270, 279–80.

Sullivan thus embodied the First Amendment's self-governance value, which emphasises that a citizen's duty to participate in the life of a democratic republic has no meaning without the freedom to express ideas and to receive expression from others.[54] Underlying this value is a commitment to the dignity of the citizen as the constant, fundamental source of all political authority. In the years before *Sullivan*, Alexander Meiklejohn had grounded the First Amendment's speech clause in a theory of self-governance, arguing that 'freedom to govern . . . implies and requires what we call "the dignity of the individual". Self-government can exist only insofar as the voters acquire the intelligence, integrity, sensitivity, and generous devotion to the general welfare that, in theory, casting a ballot is assumed to express.'[55] Citing 'the dignity of a governing citizen', Meiklejohn argued that the First Amendment should absolutely prohibit libel suits brought against speakers for attacking the fitness of public candidates.[56] A similar understanding fuelled Justice Brennan's only marginally less expansive opinion in *Sullivan*.[57] In a case pitting the wounded reputational dignity of the police commissioner against the ill-protected political dignity of his citizen-critics, the court levelled the playing field by ensuring that citizens and the press have substantial legal protection for critical comment, even for comment that turns out to be both defamatory and factually wrong. 'Dignity', then, was a value on both sides of *Sullivan*, but the dignity associated with equal participation in democratic life gave much greater force to the speech and press interests in the case.

In non-judicial writings later in his life, Justice Brennan explicitly identified 'the essential dignity and worth of each individual' as the lynchpin

[54] On the principal values animating the First Amendment liberties of speech and press, see generally Thomas I. Emerson, 'Toward a General Theory of the First Amendment' (1963) 72 *Yale Law Journal* 877. For a useful overview of the roots of the self-governance value, see Vincent Blasi, 'Learned Hand and the Self-Government Theory of the First Amendment: *Masses Publishing Co.* v. *Patten*' (1990) 61 *University of Colorado Law Review* 1.

[55] Alexander Meiklejohn, 'The First Amendment is an Absolute' [1961] *Supreme Court Review* 245 at 255.

[56] Ibid. 259.

[57] By twice invoking Madison's understanding of the citizen's censorial power – 376 US 254 at 275, 282 (1964) – by maintaining that 'it is as much [the citizen's] duty to criticize as it is the official's duty to administer' (ibid. 282) and by declaring that citizens do and must possess 'a fair equivalent of the immunity granted to [federal] officials' for speech on public matters (ibid. 282–3), Justice Brennan clearly recognised dignity in the sense of the citizen's centrality as source of power and legitimacy in the American form of government. Kalven noted that Justice Brennan 'almost literally incorporated Alexander Meiklejohn's thesis that in a democracy the citizen as ruler is our most important public official': Kalven, 'The New York Times Case', above n. 50, 209.

of American citizenship.[58] He stated that '[r]ecognition of broad and deep rights of expression and conscience reaffirm the vision of human dignity' by facilitating public debate and encouraging the development of political convictions.[59] 'The constitutional vision of human dignity', Justice Brennan wrote, 'rejects the possibility of political orthodoxy imposed from above; it respects the rights of each individual to form and to express political judgments, however far they may deviate from the mainstream and however unsettling they might be to the powerful or to the elite.'[60] This theme lent itself quite readily to the construction of a complex edifice of libel doctrine. The court fleshed out the meaning of actual malice, mandated independent judicial review of findings of constitutional fault, stymied end-runs around libel law by enterprising plaintiffs who tried to use other torts for the same purposes, and clarified differences between statements of fact and non-fact.[61]

However, the concept of participatory dignity had little to say about non-political or less clearly speech-centred dimensions of contemporary life. Thus, the argument that a 'private plaintiff' should be permitted to win a libel case by meeting a less demanding fault requirement than a public official elicited no sympathy from Justice Brennan. He disagreed with others on the court who in the late 1960s and 1970s focused on categories of plaintiffs (public or private), rather than on categories of speech (public concern or private concern). By urging that speech relating to matters of public concern should be protected under the actual malice test, without reference to plaintiff status, Justice Brennan expressed a predominating concern for the speech interests of citizen-critics and the press, as well as for the interest of citizens at large in receiving an untrammelled flow of information on public matters. As for the private realm, he believed that it was not entirely distinct from the realm of political participation and

[58] William J. Brennan Jr, 'Reason, Passion, and "The Progress of the Law"' (1988) 10 *Cardozo Law Review* 3 at 15.

[59] William J. Brennan Jr, 'The Constitution of the United States: Contemporary Ratification' (1985) 27 *South Texas Law Review* 433 at 442–3, cited in Stephen J. Wermiel, 'Law and Human Dignity: The Judicial Soul of Justice Brennan' (1998) 7 *William and Mary Bill of Rights Journal* 223 at 238–9.

[60] Ibid.

[61] *St Amant* v. *Thompson*, 390 US 727 (1968) (defining 'reckless disregard' component of actual malice); *Bose Corp.* v. *Consumers Union*, 466 US 485 (1984) (mandating de novo review of findings of actual malice); *Hustler Magazine Inc.* v. *Falwell*, 485 US 46 (1988) (adding element of actual malice to public figure suits for intentional infliction of emotional distress); *Milkovich* v. *Lorain Journal Co.*, 497 US 1 (1990) (differentiating between statement of fact and non-fact for purposes of libel).

should not be treated as if it were. 'Voluntarily or not', he wrote for the plurality in *Rosenbloom* v. *Metromedia Inc.*, 'we are all "public" men to some degree.'[62] In his view, no party seeking damages in connection with a story about a public matter should skirt the test of *Sullivan*.[63]

A majority of the court ultimately rejected Justice Brennan's idea that 'we are all "public" men to some degree', and drew a line between private and public figures for purposes of defining fault requirements in libel cases. However, it was only a line; the majority did not develop the concept of privacy in a significant way. Fuelling this majority was another strand of the self-governance value, emphasising neither the dignity of the citizen nor the dignity of private identity, but something quite different: the perception of governmental legitimacy advanced by strong legal protections of speech and press. Justice Powell voiced this second strand of the self-governance value in his opinion for the majority in *Gertz* v. *Robert Welch Inc.*,[64] where the court recognised that governmental legitimacy requires substantial tolerance of diverse ideas,[65] yet fashioned rules that were less protective of expression than the rules Justice Brennan had advocated under the citizen-dignity rationale.[66] Although the two strands emphasised quite different aspects of self-governance, *Gertz* resembled *Sullivan* in one key way: it displayed the same willingness to create legal doctrine.

[62] 403 US 29 at 48 (1971) (Brennan J) (rejecting separate fault requirements for private and public figures, and noting that 'the idea that certain "public" figures have voluntarily exposed their entire lives to public inspection, while private individuals have kept theirs carefully shrouded from public view is, at best, a legal fiction'). Elsewhere in the same opinion, Justice Brennan wrote, 'It is important to recognize that the private individual often desires press exposure either for himself, his ideas, or his causes. Constitutional adjudication must take into account the individual's interest in access to the press . . . A constitutional rule that deters the press from covering the ideas or activities of the private individual thus conceives the individual's interest too narrowly': ibid. 47 n. 15.

[63] On the other hand, the same person might be entitled to a non-damages vindication remedy in the form of a retraction of statements that have been adjudicated false and defamatory: *Rosenbloom* v. *Metromedia Inc.*, 403 US 29 at 47 n. 15 (1971). A vindication remedy would serve both the defamed individual's interest in his or her community standing, and the citizen's interest in receiving a correction of earlier-publicised, mistaken facts.

[64] 418 US 323 (1974).

[65] Ibid. 340 n. 8 (quoting Thomas Jefferson's first Inaugural Address inviting dissent even as to the republican form of government and extolling the role of reason in the competition of ideas).

[66] The *Gertz* majority revamped the common law rules for private plaintiffs in libel actions. It prohibited strict liability, 418 US 323 at 347 (1974); limited plaintiffs proving negligence to damages for actual injury, at 349–50; and forbade presumed and punitive damages absent proof of actual malice, at 350.

Following self-governance as a core jurisprudential guide, both cases produced a complex set of implementing rules.[67]

The court's first public disclosure case, *Cox Broadcasting Corp.* v. *Cohn*,[68] arose soon after *Gertz* and contained no hint of dignity as central to the plaintiff's side of the case, as if the libel cases had exhausted the concept or appropriated it substantially to the realm of political consciousness. To be sure, dignity had played a key role in the contemporaneous abortion decision,[69] and one might have expected it to migrate easily to other contexts. But, the abortion controversy dealt with the *citizen*'s dignitary right to be exempt from governmental restrictions on intimate decisions. Without a concept of personal dignity for a setting that did not involve state efforts to control intimate decisions, the court had few theoretical resources for understanding what privacy could mean in a suit concerning dissemination of intimate facts. And, by the time of *Cox Broadcasting*, the court may have been unwilling to look hard for a dignitary interest that would less compellingly launch another exercise in complex federal rule-making for a common law tort.

The court may also have sensed that dignity, even a non-political concept of dignity, did not fully capture the core value at stake in common law privacy. Perhaps the justices saw that *Sullivan*'s concept of dignity, although appropriate for considerations of equality central to that case, was essentially static in nature, and that the nature of privacy, as a process of self-realisation, was dynamic. As discussed below, the justices moved only slowly toward a sense that privacy implicates not equality of the one, speaking on a public stage, but the free interaction of the several, just off the public stage, in the flourishing of emotional and intellectual growth.

A liberty-based approach to privacy

How did this slow movement unfold? In *Cox Broadcasting*, the father of a girl who had died following a gang rape sued a television station for broadcasting the girl's name. Although a state law barred use of a rape victim's name, the reporter lawfully came across the name in court documents during the prosecution of the girl's attackers. The court held that a state may not impose sanctions on the accurate publication of information obtained from judicial records that were available for public

[67] For the classic treatment of the court's democracy-promoting function, see John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review* (Cambridge, Mass.: Harvard University Press, 1980).

[68] 420 US 469 (1975). [69] *Roe* v. *Wade*, 410 US 113 (1973).

inspection in the course of a public prosecution.[70] The court cast no light on common law privacy, perhaps because the plaintiff was the father of the deceased girl, not the victim herself, and his interest was vague at best. The lower court's opinion had summarised the father's puzzling claim: that public disclosure of his daughter's name 'intruded upon his right to be left alone, free from and unconnected with the sad and unpleasant event that had previously occurred'.[71] It would not be unreasonable to interpret this claim as the father's right to disconnect himself from the crime, as if the 'event' of his daughter's rape and death could be wished away. An interest in fleeing the reality of a very recent, publicised, and prosecuted crime could have little or no weight, especially when the victim's name appeared in court documents.[72] The Supreme Court's narrow ruling left open the possibility that a more plausibly defined privacy claim could fare differently in a future case.

However, the court's second case, another dispute over naming a rape victim, was not much more enlightening. In *The Florida Star* v. *BJF*,[73] a sheriff's department inadvertently included the name of a rape victim in an incident report that was made publicly available in the department's pressroom. A newspaper's trainee gathered the information, and the paper published the name in mistaken violation of its own policy. In a civil action based on a state misdemeanour statute, the victim invoked her own interest in freedom from distressing publicity about her experience of rape. She also sought to differentiate her case from *Cox Broadcasting* by asserting an interest in physical security. In the wake of the newspaper's account of the assault, she had received threatening calls, possibly from the rapist,[74] causing her 'to change her phone number and residence, to seek police

[70] *Cox Broadcasting Corp.* v. *Cohn*, 420 US 469 at 490–5 (1975).

[71] *Cox Broadcasting Corp.* v. *Cohn*, 200 SE 2d 127 (Ga. 1973).

[72] '[G]enerally, as with defamation and false light claims, . . . recovery for the invasion of a family member or friend's privacy, is not recognized', Sack, *Sack on Defamation*, above n. 4, pp. 12–35, although authority exists for a parent's independent privacy interest in non-publication of photographs of a deceased child or family member: see *Reid* v. *Pierce County*, 961 P 2d 333 (Wash. 1998). In a case interpreting the personal privacy exemption of the Freedom of Information Act, 5 USC s. 552(b)(7)(c), the US Supreme Court recognised a surviving family's privacy interest in non-disclosure of death-scene photographs of a deceased family member who had served in the Clinton White House: *National Archives and Records Admininstration* v. *Favish*, 541 US 157 (2004). The court observed generally that the 'the statutory privacy right protected by Exemption 7(C) goes beyond the common law and the Constitution': 541 US 157 at 170 (2004) (citing *Department of Justice* v. *Reporters Committee for Freedom of the Press*, 489 US 749 at 762 n. 13 (1989)).

[73] 491 US 524 (1989). [74] Ibid. 528.

protection, and to obtain mental health counseling'.[75] Although a jury awarded her compensatory and punitive damages, BJF's claim fared no better in the US Supreme Court than the father's claim in *Cox Broadcasting*. To be sure, the Supreme Court credited as 'highly significant' three interests supporting the suit: the 'privacy of victims of sexual offences; the physical safety of such victims, who may be targeted for retaliation if their names become known to their assailants; and the goal of encouraging victims of such crimes to report these offenses without fear of exposure'.[76] However, the court ruled that the action for damages was insufficiently tailored to justify 'the extraordinary measure'[77] of punishing the publication of truthful information lawfully obtained from a government record. According to the court, it would be anomalous to hold the press responsible for the government's failure to keep the information secure; moreover, because BJF's statutory remedy lacked several of the elements of the common law public disclosure tort, recovery was too 'automatic' to satisfy the First Amendment.[78] The court found a public interest in favour of transparency of records made available to the public, and against saddling reporters with a duty to sift such records for invasiveness.[79] The court added that it might recognise in a future case a 'zone of personal privacy within which the State may protect the individual from intrusion by the press',[80] but the court offered no hint about the kind of facts that would qualify.

Lower courts following the lead of *Cox Broadcasting* and *Florida Star* have avoided critical reflection on common law privacy and have opted for result-driven emphasis on the use of government records. A dramatic recent example is *Gates* v. *Discovery Communications, Inc.*,[81] where the California Supreme Court dismissed a public disclosure case brought against makers of a documentary that revisited a ten-year-old crime and identified its participants. One of the participants, the plaintiff, had pled guilty to a felony, completed a prison term, and subsequently settled into 'an obscure, lawful life', becoming 'a respected member of the community'.[82] The documentary, he argued, exposed his past and unreasonably disrupted his new life. Citing the rape victim cases and other precedents, the court reaffirmed the First Amendment's protection of truthful reporting of information found in 'public (i.e., not sealed) official records', and

[75] Ibid. [76] Ibid. 537. [77] Ibid. 540.
[78] Ibid. 535, 538–9. [79] Ibid. 535–6. [80] Ibid. 541.
[81] 101 P 3d 552 (Cal. 2004) (overruling *Briscoe* v. *Reader's Digest Association, Inc.*, 483 P 2d 34 (Cal. 1971)).
[82] Ibid. 554.

noted that the relevant precedents 'neither logically nor practically lend themselves to temporal limitation'.[83] Accurate disclosures from records of yesteryear therefore enjoy the same privilege as disclosures drawn from contemporary judicial proceedings and comparable public sources, seemingly regardless of the privacy interest at stake.

Even if a statute prohibits the government from releasing highly sensitive materials, such as juvenile arrest records, it appears that the press loses no right to publish their contents when lawfully received. In *Bowley* v. *Uniontown Police Department*,[84] a federal appeals court dismissed a public disclosure case brought against a newspaper for naming a juvenile who had been arrested in the rape of a child. A statute prohibited officials from disclosing information in juvenile arrest records but did not make it unlawful to receive the information. In the court's view, then, the case involved a government entity whose stewardship of information went awry, and a newspaper that innocently gathered and published facts of legitimate public concern. On this characterisation of the case, imposing damages on the press was an insufficiently tailored means of protecting the juvenile; the proper solution would have been non-release by the government in the first place. This logic enabled the court to bypass any consideration whatsoever of the sufficiency of the juvenile's interest in privacy.

The Colorado Supreme Court gave greater attention to privacy in *In re People* v. *Bryant*[85] – but it was perhaps too much attention with too little analysis. In a sensational criminal case involving an allegation of rape against a celebrity athlete, the court unexpectedly upheld a prior restraint against the press and justified the order on privacy grounds. Pursuant to the state's rape shield law, the victim had testified in a closed pre-trial hearing to determine the relevance and admissibility of evidence concerning any sexual activities she engaged in just before and after the alleged rape.[86] A court reporter accidentally sent transcripts of the 'intensely private and personal'[87] sealed testimony to members of the press. When the error was discovered, the trial judge ordered the press not to publish the contents. The press then petitioned the state supreme court to invalidate this extraordinary restraint on information that the press had done nothing wrong to obtain and that the court itself had delivered into the press's hands. In a 4–3 decision, the high court ruled that the victim's privacy

[83] Ibid. 555, 561–2. [84] 2005 WL 948842 (3rd Cir. 2005).
[85] 94 P 3d 624 (Col. 2004). [86] Ibid. 626. [87] Ibid. 635.

interests were of the highest order[88] and that a carefully tailored prior restraint met the First Amendment's most unforgiving requirements.[89] Though daring, the decision will likely have minor impact on the law's consideration of privacy. First, the court unpersuasively relied on authorities that neither involved prior restraints nor upheld privacy interests in damages actions. Second, the court failed to treat adequately the point (stressed by a strong dissent) that, because most of the 'private' information about the victim had already appeared in public court documents, the order could not be effective.[90] Third, although the decision evidenced understandable compassion for the victim and any future complainant whose rape shield testimony reaches the public domain, the court offered nothing conceptually new about the meaning of privacy and arguably nothing on the facts that could warrant a prior restraint. Ultimately, *Bryant* may be considered a product of its unique circumstances, including the stricken court's sense that it had run out of options to cure its own error.

It took the US Supreme Court's decision in *Bartnicki* v. *Vopper*[91] to offer seeds of richer thinking about privacy. The case involved not the common law tort but a statutory cause of action brought by union officials whose private cell-phone conversation about a contentious labour negotiation was intercepted by an unknown person. The interceptor handed a tape of the call to an anti-union figure, who leaked it to a talk-radio host, who played it over the air some months later.[92] The union officials sued the radio host, among others, under federal and state statutory provisions aimed at protecting the privacy of electronic communications.[93] Once the plaintiffs successfully resisted summary judgment at the trial level, the question before the court was whether the First Amendment prohibited

[88] The Colorado Supreme Court cited three interests: protecting victims' privacy, encouraging victims to report sexual assault, and furthering the prosecution and deterrence of sexual assault: ibid. 632.

[89] The high court ordered the trial judge to rule expeditiously on the admissibility of evidence under the rape shield law and to consider public release of transcripts containing portions that were relevant and material to the case: ibid. 638. Soon after, the trial judge ruled that 'much of the material in the hearing could be made public', Rodney A. Smolla, *Smolla & Nimmer on Freedom of Speech* (3rd edn, New York: Clark Boardman Callaghan, 1996–2005) [15:33.50], as Justice Breyer had anticipated when the media sought a stay of the original order, *Associated Press* v. *District Court*, 125 S. Ct 1 (2004) (denying application for stay). The prosecution was ultimately dropped.

[90] *In re People v. Bryant*, 94 P 3d 624 at 642–4 (Col. 2004) (Bender J dissenting).

[91] 532 US 514 (2001).

[92] Ibid. 518–19.

[93] Ibid. 523–4 (summarising relevant provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968).

imposing civil damages for disclosure of an illegally intercepted telephone conversation. The case was complicated by the fact that the conversation included angry remarks about the plaintiffs' opponents in the labour dispute, including seemingly hyperbolic statements about doing violence to them.[94]

In an opinion for a six-member majority, Justice Stevens concluded that the intercepted conversation addressed a matter of public concern and that the statutory provisions therefore were unconstitutional as applied.[95] This familiar protection of speech deemed 'public' placed *Bartnicki* in the long line of *Sullivan*-driven, dignity-based speech decisions of the Supreme Court: Justice Stevens implicitly extolled both the media's right to disseminate speech relevant to civic needs, and the citizen's right to receive the speech in the exercise of self-rule. However, there was more to *Bartnicki* than the familiar. Justice Stevens' comments about the other side of the case, particularly his recognition of the plaintiffs' speech-based interest in privacy, made the case distinctive. 'Privacy of communication is an important interest', the justice wrote, and 'the fear of public disclosure of private conversations might well have a chilling effect on private speech'.[96] Justice Stevens thus established that private speech is constitutionally significant, indeed part of 'the constitutional calculus', and that when private and public speech clash, the calculus reveals a tension not often noted by judges or parties. However, without further elaboration of the nature or value of private speech, he concluded that, on the scales of the First Amendment, public airing of the conversation outweighed the plaintiffs' interest in keeping it confidential. Justice Stevens ignored the possibility that private dialogue about a public issue could well have stronger significance for the speakers – and serve greater social purpose – than speech about the same issue addressed to a general public over the airwaves.[97]

Justice Breyer's concurring opinion, joined by Justice O'Connor, underscored the majority's insight that privacy can have an important speech component. Justice Breyer strongly suggested that the analogous public disclosure tort was neither dead nor obsolete, and he declared that courts

[94] Smolla correctly questions whether some of the justices who ruled for the defendants took the cell-phone conversation too literally: Smolla, 'Information as Contraband', above n. 20, 1144.

[95] *Bartnicki* v. *Vopper*, 532 US 514 at 534 (2001). [96] Ibid. 532–3.

[97] Ibid. 535. Discussing the majority opinion's 'nods to privacy', Smolla calls them 'perfunctory and obligatory, if not downright miserly': Smolla, 'Information as Contraband', above n. 20, 1141.

should eschew 'rigid constitutional rules' in adjudicating clashes between privacy and the claims of new information-gathering technologies.[98] On the facts of *Bartnicki*, Justice Breyer rejected a simplistic 'public interest' exception to the statutory protections of privacy, but he concurred in the majority's conclusion, viewing the case as involving 'unusually low privacy expectations' on the part of the plaintiffs, and an 'unusually high' public interest in broad dissemination of the violence-tinged conversations.[99] Justice Rehnquist's dissent rejected First Amendment protection for the statutory violations, whether the intercepted conversation addressed a public issue or not.[100]

Bartnicki broke ground by associating privacy with speech and withholding any sort of presumptive privilege for media disclosure of private electronic conversations.[101] The case intimated that privacy is relational, that its core consists of freedom to interact with others in a certain way for a certain purpose. It is important now to follow these hints and to consider more deeply the relational aspects of contemporary life's private dimension.

Today a sizeable body of writing about 'the modern self and its predicament'[102] can assist in filling in conceptual gaps of the privacy tort. For example, just as the court in libel cases took important cues from Meiklejohn to illuminate a political concept of human dignity,[103] legal thought today may profit from the writings of Richard Rorty on the development of the person.[104] Offering a 'way of looking at human beings',[105] Rorty draws on a number of potent sources: the ethic of self-creation associated with nineteenth-century essayist Ralph Waldo Emerson;[106] John Dewey's

[98] *Bartnicki* v. *Vopper*, 532 US 514 at 537, 540–1 (2001) (Breyer J concurring).

[99] Ibid. 540. [100] Ibid. 554–5 (Rehnquist CJ dissenting).

[101] Despite the plaintiffs' loss, Smolla aptly calls *Bartnicki* 'a backhanded victory' for privacy: Smolla, 'Information as Contraband', above n. 20, 1150.

[102] Stephen K. White, *Sustaining Affirmation: The Strengths of Weak Ontology in Political Theory* (Princeton: Princeton University Press, 2000) p. 63.

[103] See William J. Brennan Jr, 'The Supreme Court and the Meiklejohn Interpretation of the First Amendment' (1965) 79 *Harvard Law Review* 1.

[104] Richard Rorty, 'Freud and Moral Reflection' in Joseph H. Smith and William Kerrigan (eds.), *Pragmatism's Freud* (Baltimore: Johns Hopkins University Press, 1986); Richard Rorty, 'The Contingency of Selfhood' in *Contingency, Irony, and Solidarity* (Cambridge: Cambridge University Press, 1989).

[105] Rorty, 'Contingency of Selfhood', above n. 104, 35. For a judge's reflection on the judiciary's obligation in hard cases 'not to define humanity, but to describe and recognize it', see Jeffrey L. Amestoy, 'Uncommon Humanity: Reflections on Judging in a Post-Human Era' (2003) 78 *New York University Law Review* 1581.

[106] Rorty sees Emerson as 'not a philosopher of democracy but of private self-creation': Richard Rorty, *Philosphy and Social Hope* (London: Penguin, 1999) p. 26.

broad concept of education as 'a constant reorganizing or reconstructing of experience' for the purpose of personal growth;[107] and Freud's concept of 'private morality', meaning the part of existence pertaining less to issues of justice and more to the self's own search for character.[108] What interests Rorty is the 'attempt of individuals to be reconciled with themselves',[109] through a process of engaging in 'what Freud considered the most difficult of all personal accomplishments: a genuinely stable character in an unstable time'.[110] This search does not imitate the ancient Greek pursuit of essential human nature but entails a recognition of the self as a 'web of relations',[111] and an understanding of growth as the self's adaptation to the 'sheer contingency of individual existence'.[112] How is adaptation achieved and a sense of identity forged? Rorty connects identity to an ability to define, in one's own speech, 'the causes of our being what we are', not accepting 'somebody else's description' but 'sketch[ing] a narrative' of our development and creating a self out of 'the contingencies of our upbringing'.[113] In this sense, 'the self continually attempts to construct a narrative about its place in the world'.[114] Such a narrative enables us 'to make something worthwhile out of ourselves, to create present selves whom we can respect'.[115] Rorty's Freud would define freedom as the self's 'recognition of contingency', and he would define failure as an inability to 'break free from an idiosyncratic past'.[116]

This view of self-development crucially depends on articulating a narrative of one's past. One of Rorty's contemporaries, the philosopher Charles Taylor, has argued that the process of self-definition is inherently dialogic, a conversational engagement with one's past and with others.[117] For Taylor, self-definition is possible only through 'dialogue with, and sometimes in struggle against, the identities our significant others want to recognize in us'.[118] In a complex body of work, Taylor has explored the 'ideal of authenticity' underlying self-realisation in Western character.

[107] John Dewey, *Democracy and Education* (New York: Macmillan, 1961) p. 76.
[108] Rorty, 'Moral Reflection', above n. 104, 10–11. [109] Ibid. 11. [110] Ibid. 9.
[111] Rorty, *Philosophy and Social Hope*, above n. 106, p. 53.
[112] Rorty, 'The Contingency of Selfhood', above n.104, 26. [113] Ibid. 27–32.
[114] Richard H. King, 'Self-Realization and Solidarity: Rorty and the Judging Self' in Smith and Kerrigan (eds.), *Pragmatism's Freud*, above n.104, p. 38.
[115] Rorty, 'The Contingency of Selfhood', above n. 104, 33. [116] Ibid.
[117] Of course, Rorty and Taylor disagree on various aspects of moral experience, and they have engaged in a long-running exchange. See, e.g., Richard Rorty, 'Taylor on Truth' in James Tully (ed.), *Philosophy in an Age of Pluralism* (Cambridge: Cambridge University Press, 1994). Those disagreements are not pertinent here.
[118] Charles Taylor, *The Ethics of Authenticity* (Cambridge, Mass.: Harvard University Press, 1992) p. 33.

The ideal stems from the 'idea that each of us has an original way of being human', that 'I am called upon to live my life in this way, and not in imitation of anyone else's'.[119] Dialogue, 'partly overt, partly internalized', makes possible the discovery of one's own way.[120] Like Rorty, who argued that the recognition of contingency defined freedom,[121] Taylor sees authenticity as an idea of freedom.[122] For both, freedom is the self's power to define and create an individual path.

These reflections combine well with a strain of American jurisprudence that takes self-determination to be the core meaning of liberty. John L. Hill has argued that the ideal of freedom in American political and legal consciousness transcends negative and positive liberty as a third concept altogether, marked in part by a strong emphasis on privacy as a means of self-determination.[123] To the extent that the law recognises that 'the self must be protected from the great levelling force of social influences that threaten to submerge it', the interest in privacy is negative; to the extent that the law protects privacy as a means of encouraging growth, development, and ultimately participation in society, the interest is essentially positive.[124] Hill concurs that the self's participation with others – its unfettered 'connection with smaller groups and associations' – can be central to the formation of identity.[125]

These sources lead to a conclusion that the three-sided model of a privacy dispute may be erroneous. It should no longer be possible to say that a privacy suit involves only a complainant, a disclosing entity (usually a media outlet), and the public recipient of the media's information (the electorate, always ready to receive information of public concern). A more textured account of privacy would hold that the model has four sides: a complainant, a disclosing entity, recipients of the information, and the complainant's intimate group of associates. This is the circle that Rorty, Taylor, and Hill would see as the facilitating dialogic milieu in which the self learns to separate from an 'idiosyncratic past' and forge its own stable identity. Media dissemination of highly personal details arguably disrupts the freedom of close interaction between the complainant and the group by shocking their relationships with previously unknown facts, or

[119] Ibid. pp. 28–9. [120] Ibid. p. 47.
[121] Rorty, 'The Contingency of Selfhood', above n. 104, 33.
[122] Taylor, *Ethics of Authenticity*, above n. 118, pp. 67–8.
[123] John L. Hill, 'A Third Theory of Liberty: The Evolution of Our Conception of Freedom in American Constitutional Thought' (2002) 29 *Hastings Constitutional Law Quarterly* 115.
[124] Ibid. 173. [125] Ibid. 174.

pre-empting the complainant's ability to bring the facts into the conversation on his or her own terms, in his or her own time. If growth takes place within a zone of dialogue and facilitating ties, the risks of injuring relationships within that zone can be substantial.

Some plaintiffs have come close to presenting an interest of this kind. In public disclosure cases not involving the media, several US jurisdictions recognise damage to 'special relationships' as a substitute for the publicity element of a plaintiff's case.[126] This chapter proposes that, in media cases where the publicity element has been met, such damage should be central to the law's understanding of the nature of the privacy interest. In *Sidis*, for example, the ex-prodigy interacted with a very small circle whose support clearly nurtured his effort to 'break free from [an] idiosyncratic past'.[127] His complaint alleged that the *New Yorker*'s article tracing his early public life, his subsequent revulsion and desire for obscurity, and his odd fate as an adult, caused him 'grievous mental anguish', specifically that 'for a long time to come [he] will be severely damaged and handicapped in his employment as a clerk or in any other employment and in his social life and pursuit of happiness'.[128] In the latter phrase, Sidis may have been struggling to articulate an idea of disrupted pivotal relationships.[129] Perhaps Sidis lost his case in part because the court lacked understanding that his principal harm was relational – an impairment of the freedom to interact with people of his choice, on his own terms, in a zone made safe for personal development.[130]

[126] E.g., *Hill* v. *MCI WorldCom Communications Inc.*, 141 F Supp. 2d 1205 (SD Iowa 2001), *Beaumont* v. *Brown*, 257 NW 2d 522 (Mich. 1977).

[127] Rorty, 'The Contingency of Selfhood', above n. 104, 33. A popular biography of Sidis, including the story of his efforts to move beyond his parental influence, is Amy Wallace, *The Prodigy* (New York: E. P. Dutton, 1986).

[128] Wallace, *The Prodigy*, above n. 127, p. 234.

[129] On Sidis' few friendships, see Wallace, *The Prodigy*, ibid. p. 222. A poem by Philip Larkin, 'Nothing significant was really said', echoes the story of the American prodigy. In the poem, a 'brilliant freshman' has given a public talk, presumably at a university, and has been acclaimed a 'genius', as in Sidis' life: see Wallace, *The Prodigy*, ibid. pp. 59–60. But Larkin writes that one who had heard the brilliant talk had 'found the genius crying when alone' and saying, 'O what unlucky streak/ Twisting inside me, made me break the line?/ What was the rock my gliding childhood struck,/ And what bright unreal path has led me here?' Philip Larkin (with introduction by A. Thwaite), *Collected Poems* (London: Marvell/Faber and Faber, 1988) p. 235.

[130] Other cases contain traces of a theory of disrupted personal relationships necessary for growth, e.g., *Howard* v. *Des Moines Register & Tribune Co.*, 283 NW 2d 289 at 292 (Iowa 1979), in which a teenager who was involuntarily sterilised at a county home claimed that before a newspaper publicised her name and condition, 'she led a quiet and respectable life and made friends and acquaintances who were not aware of her surgery'. She alleged that

The plaintiffs in *Hall* v. *Post*[131] may have argued along similar lines. A newspaper reported the local arrival of a woman seeking the daughter that she had left behind seventeen years earlier. The news story helped the birth mother locate Mary Hall, who had adopted the child, and led to a confrontation by telephone between the two mothers. A follow-up story included the names of Mary Hall and the adoptive child, related the 'emotional telephone encounter' between the mothers, and 'dwelt heavily upon the emotions of both families – the [birth family's] joy and desire to see [the daughter], and the distress, shock, and fear of the [adoptive family]'.[132]

In a suit for public disclosure, Mary Hall included a claim for 'intrusion into [the family's] private affairs and solitude', which the court associated with another cause of action, the intrusion tort of the *Restatement (Second) of Torts*.[133] However, Hall may have been alleging something other than that trespass-related action. 'Intrusion' for Hall may have referred to harm to intimate associations, including family and other relationships, caused by the newspaper's report of the facts of the adoption and the mothers' exchange. Publicity forces private persons to address history that they would not otherwise address, or forces them to confront matters at a time or in a context that they would not choose. Publicity also pre-empts the first telling of facts; despite a plaintiff's best efforts, it may be impossible to dislodge a media account from the minds of those whose support is crucial yet perhaps imperfect and subject to outside influence. The plaintiffs in *Hall* v. *Post* may have meant to capture these or other concerns in their claim of 'intrusion,' but the argument was too indirect to be heard by the court.[134]

the story 'subjected her to 'public contempt, humiliation, and "inquisitive notice"'. For a valuable discussion linking privacy to John Stuart Mill's concept of human flourishing, see Megan Richardson, 'Whither Breach of Confidence: A Right of Privacy for Australia' (2002) 26 *Melbourne University Law Review* 381 at 388–93. For an interesting analysis of the importance of confidentiality for the 'maintenance of relationships critical to self-realization', see David F. Partlett, 'Misuse of Genetic Information: The Common Law and Professionals' Liability' (2003) 42 *Washburn Law Journal* 489 at 502 (noting that '[o]rganization of human and communal affairs depends upon individuals' willingness to enter cooperative relationships with one another').

131 372 SE 2d 711 (NC 1988).

132 *Hall* v. *Post*, 355 SE 2d 819 at 822 (NC Ct App. 1987).

133 Ibid. 823.

134 The North Carolina Supreme Court dismissed the 'intrusion' claim: ibid. The court also chose not to recognise the public disclosure tort, stating that the action would create tension with freedoms of speech and press, and that it overlapped substantially with the

A changed tort?

Several doctrinal implications flow from a concept of privacy as liberty to develop character through close, dialogic relationships with others. The following proposals are ordered in terms of the extent to which they depart from the status quo. The first proposal involves least change in existing doctrine, the second moves further beyond the status quo, and so forth.

Nexus test

What follows if courts accept the idea that harm in a privacy case can be more significant than usually acknowledged, in that the media's dissemination of intimate facts can burden private speech, impairing the individual's ability to develop character through dialogic exchange? Would the courts consider altering existing doctrine to reflect a more evenly struck balance of interests? At present, the most difficult requirement for plaintiffs is the showing that a disclosure bears no connection to a 'matter of legitimate public concern'. Courts usually err on the side of the media on this issue, granting summary judgment if any reasonable editor could find a substantial nexus between the intimate fact and a public matter.[135] However, where the constitutional calculus involves private speech, and the value of that speech for freedom of self-development is recognised, favouring media defendants so dramatically on the nexus question is no longer justified. The test should be whether reasonable editors could differ on the existence of a substantial nexus between the intimate fact and the public matter. If they could differ, the question should go to the jury.

Thus, in *Hall* v. *Post*, where the newspaper printed details of the emotional collision between two mothers in a telephone conversation, the details of the conversation would likely be considered private facts. Whether they related to a matter of public concern – the workings of state adoption policies – should surely be left to the judgment of a jury.

action for intentional infliction of emotional distress: *Hall* v. *Post*, 372 SE 2d 711 at 714–17 (NC 1988). The court speculated that plaintiffs 'could more easily establish a claim' under the already recognised intentional infliction tort than under the public disclosure tort: ibid. 716–17. For discussion of the intentional infliction tort, see generally Dan B. Dobbs, *The Law of Torts* (St Paul, Minn.: West, 2000) pp. 824–35.

[135] E.g., *Gilbert* v. *Medical Economics Co.*, 665 F 2d 305 (10th Cir. 1981).

Public controversy/duty to notify requirements

Under the existing public disclosure tort, matters of 'legitimate public concern' need not predate the story in question and arguably include almost anything that the media decides to publish. As a result, the media are free to publish facts that plaintiffs cannot see coming. Plaintiffs therefore lack the opportunity to forewarn their intimate circles that private disclosures are imminent or to address the details in advance of publication. These relationships are more likely to be disrupted if such forewarning is absent and a shocking story appears.

The tort would incorporate the plaintiff's relational interest more fairly if the defendant's privilege depended not on the broad category of 'legitimate public concern' but on a narrower category of pre-existing public controversy.[136] This category is familiar from libel law. If the tort were revised in that way, and if the plaintiff proved that the defendant gave publicity to private facts that were highly offensive to a reasonable person and involved no matter of pre-existing public controversy, then the plaintiff would prevail. In effect, the plaintiff would be arguing, 'There was no public controversy, so I had no notice of the need to confer with the persons whose support is crucial to me, and the disclosures have impaired my ability to continue these relationships.'

On the other hand, if a related public controversy has preceded the media's disclosure, arguably the existence of the controversy has provided the plaintiff an advance opportunity to discuss relevant intimate facts with a close circle, or otherwise to prepare them for eventual disclosures. Given that the plaintiff has had such an opportunity, the media rightfully can claim a privilege to disclose intimate facts substantially related to the public controversy.[137]

If a media outlet wishes to publish a story containing intimate facts about a private person, and the story involves a matter of public concern, but no pre-existing public controversy, does the outlet publish at its risk? Civil liability appears harsh in view of constitutional interests of speech and press, even with a new understanding of the role of private, dialogic

[136] In libel cases, a limited purpose public figure is defined in part as one who has voluntarily injected him or herself into a public controversy: *Gertz*, 418 US 323 at 345 (1974). A public controversy 'is not simply a matter of interest to the public; it must be a real dispute, the outcome of which affects the general public or some segment of it in an appreciable way': *Waldbaum* v. *Fairchild Publications Inc.*, 627 F 2d 1287 at 1296 (DC Cir. 1980).

[137] Smolla has made a similar proposal for somewhat different reasons: Smolla, 'American Privacy Law', above n. 3, 300–1.

relationships in the growth of the person and the harm posed by media dissemination. In these circumstances, courts should consider imposing on the media a duty to inform the private person of an imminent invasive disclosure. This information would afford a private person the same opportunity of advance contact with an intimate circle that the private person would have in the context of a pre-existing public controversy. A media entity's satisfaction of this duty to notify would eliminate the possibility of punitive damages, and should be relevant to the amount of compensatory damages. It would not automatically eliminate compensatory damages, however, because the disclosures were not substantially related to a pre-existing public controversy.

An example would come from *Sidis*. The court held that the magazine profile of the prodigy involved a matter of public concern,[138] but did it involve a pre-existing controversy? The author, noted writer James Thurber, thought that the story involved the social issue of whether parents should thrust their talented children so forcibly into the limelight. Thurber was disturbed that the court did not understand this.[139] It may be that a jury would understand it no better and would find that the topic of parental pressure was not a 'controversy' in the law's sense of a 'real dispute'.[140] The jury would award damages, not needing to reach the further question of whether details in the story – including depictions of the plaintiff's personal hygiene, bedroom, and odd behaviour – satisfied the nexus requirement addressed above. If the defendant had given the plaintiff advance notification of the story, no punitive damages would be available and compensatory damages might be reduced. If on the other hand, the jury did find a pre-existing public controversy, and found that some or all of the intimate disclosures reasonably related to the controversy, Sidis would lose as to those disclosures.

Revised action for intentional infliction of emotional distress

If courts wish greater change, a third alternative would be to reject the public disclosure tort and turn to the action for intentional/reckless infliction of emotional distress as the vehicle for disclosure suits against the media. A proper balance, of course, would need to be struck between the opposing interests. Arguably, the scienter element in the intentional/reckless

[138] *Sidis* v. *F-R Publishing Corporation*, 113 F 2d 806 at 809 (2nd Cir. 1940).
[139] Wallace, *The Prodigy*, above n. 127, p. 236. [140] See above n. 136.

infliction tort would be defined as conscious disregard of a high probability that publication of intimate facts would impinge materially on the plaintiff's emotional health. The element of 'outrageous conduct' would involve analysis of whether the published information at issue lacked a plausible nexus to a pre-existing public controversy. The injury element would be met by evidence of severe emotional distress, caused by both disrupted personal relationships and other effects of disclosure.

How would this remedy fare on the facts of *Sidis*? The *New Yorker* story reflected its author's awareness of Sidis' social isolation and reliance on a small set of crucial relationships; the scienter element, therefore, could well be resolved against the defendant. The element of outrageous conduct would depend on a jury's grappling with whether a specific controversy pre-dated the profile and if so, whether the story's details substantially related to the controversy. Probably this element would also be resolved against the defendant. Finally, the element of severe emotional distress would not be difficult to prove, especially given the plaintiff's troubled emotional history, which the story itself recounted. As predicted in *Hall* v. *Post*,[141] the intentional infliction tort may be an easier claim for plaintiffs to prove, and thus unsatisfactory as a matter of policy.[142] Then again, few cases will have the factual configuration of *Sidis*, particularly the defendant's extensive knowledge of the plaintiff's history and emotional fragility.

Conclusion

Although the public disclosure tort has had an unpromising past, it appeals to what Anthony Lewis suggests is a sense of basic fairness to 'those who have not sought power' but have become illustrations of public issues. The tort's weakness may be a function of cultural indifference or constitutional qualms, although the most likely explanation is institutional: until recently, the Supreme Court offered no illumination of a core interest. Libel law had reserved the obvious candidate, dignity, for civic contexts. Now, with the court's decision in *Bartnicki* and the insights of a

[141] 355 SE 2d 819 at 822 (NC Ct App. 1987).

[142] For a case in which the court dismissed a public disclosure claim but declined on the same facts to dismiss a claim of intentional infliction of emotional distress, see *Armstrong* v. *H & C Communications Inc.*, 575 So 2d 280 (Fla. Dist Ct App. 1991). It remains to be seen whether the Supreme Court will constitutionalise actions brought by private plaintiffs under this tort, as it did in actions brought by public figures: see *Hustler* v. *Falwell*, 485 US 46 (1988).

number of contemporary thinkers, it may be time to recognise privacy as a dynamic concept involving the self's interest in growth through unhampered dialogic exchange. At the core of a reconsidered tort should be an idea of freedom – to engage in a 'web' of secure relationships that promote an essential task of human experience: creating what Rorty called 'stable character in an unstable time'.

4

The internet and private life in Europe: Risks and aspirations

YVES POULLET WITH THE COOPERATION OF J. MARC DINANT

Introduction

The reach of the internet grows day by day. Currently there are over 2 billion users and the number continues to rise. The services offered on the internet follow the same exponential trend. Electronic commerce promises ever more varied and ingenious applications, putting the world at one's fingertip with a simple click. Nevertheless concerns have been raised about this virtual universe bringing about the end of our freedoms, especially with respect to privacy. The purpose of this chapter is to bring clarity to the debate and to offer some suggestions. The topic is a timely one in Europe. There are now two European Directives on privacy protection, in particular the general Data Protection Directive 95/46/EC of 24 October 1995[1] and the more specific Privacy and Electronic Communications Directive 2002/58/EC of 12 July 2002.[2] The latter replaces the Directive 97/66/EC of 15 December 1997 on the processing of personal

This chapter is a deeply updated version of an article by the first author originally published in the French language under the title 'Internet et Vie Privée: Entre Risques et Espoirs' in (2001) *Journal des Tribunaux* 155. Translation, Dr Martin Vranken, Law Faculty, University of Melbourne. It also takes into account the report prepared by the two authors for the Council of Europe Consultative Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Yves Poullet and J. Marc Dinant, *Information Self-Determination in the Internet Era: Thoughts on Convention No. 108 for the Purposes of the Future Work of the Consultative Committee*, 13 December 2004 (T-PD (2004) 04 final).

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995, *OJ*, L 281, 23 November 1995.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002, *OJ*, L 201, 31 July 2002. On that directive, see Sophie Louveaux and Maria Veronica Perez-Asinari, 'New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communication

data and the protection of privacy in the telecommunications sector.[3] A large number of documents generated within the European Community also are topical – including the European Parliament's 1999 report on Echelon;[4] the European Commission's consultation paper on the surveillance by companies of employee internet use;[5] the European Commission's communication on spam;[6] and finally the Council Framework Draft Decision on Data Retention.[7] In addition, one has to mention the important work done by the Article 29 Data Protection Working Party on various privacy issues in order to harmonise the different national approaches.[8]

Which specific characteristics of the network account for the current controversy surrounding the internet and privacy?[9] Five features in

Sector – Some Initial Remarks' (2003) 6(5) *Computer and Telecommunications Law Review* 133.

[3] Directive 1997/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, *OJ*, L 024, 30 January 1998.

[4] European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system)*, 2001/2098(INI).

[5] European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (30 October 2002). See also EIRO (European Industrial Relations Observatory Online), Catherine Delbar, Marinette Mormont and Marie Schots, *Comparative Report on New Technology and Respect for Privacy at the Workplace*, TN0307101S, 12 August 2003, available from http://www.eiro.eurofound.ie/index.html.

[6] European Commission, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Unsolicited Commercial Communications or 'Spam'*, COM(2004) 28, 22 January 2004.

[7] Council of Europe, *Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the Purpose of Prevention, Investigation, Detection and Prosecution of Crime and Criminal Offences including Terrorism*, 8958/04, CRIMORG 36, TELECOM 82, 28 April 2004. This draft intends to harmonise in the context of the third pillar the European national regulation on traffic data retention for criminal investigation purposes.

[8] This group – commonly known as the Article 29 Working Party – was set up under Directive 95/46/EC, Art. 29 as an independent European advisory body compounded by representatives of the different national data protection authorities. Its report covers the years 2002 and 2003: European Commission, *Seventh Report on the Situation regarding the Protection of Individuals with regard to the Processing of Personal Data and Privacy in the European Union and in Third Countries* (Luxembourg: Office for Official Publications of the European Communities, 2004) (report adopted on 21 June 2004).

[9] In the context of this chapter, we do not take into consideration the development of new terminal equipment like Radio Frequency Identifier (RFID) which are very small chips embedded in goods (e.g. shirts or razors) or human beings and permit the tracking of their movements. About this new phenomenon and the new privacy threats linked with their use, see Article 29 Working Party, *Working Document on Data Protection Issues related to RFID Technology*, 10107/05/EN, WP 105, 19 January 2005.

particular stand out and warrant close attention.[10] First, there is the interactive nature of the internet, which over time leads to the generation of a vast array of person-specific information. As internet use is interactive and increasingly a part of everyday life, users themselves are the primary creators of data, whenever they enter into a dialogue with a particular website, when driving their car equipped with a global positioning system, or simply when using a mobile phone linked to the internet. All such activities leave traces, made consciously or unconsciously, and these are captured by others in order to enrich or even create various applications. Further, because of the interactive nature of the internet, users can make choices at all times: by discontinuing their visit to a particular site; by choosing whether or not to identify themselves; by insisting on this or that protection; by consenting to this or that treatment. Consent is the corollary of interactivity. It constitutes a major factor in the safeguarding of our freedoms on the internet, a point I will come back to later in this chapter.[11]

The second characteristic is the combination of flow rate and processing power increase. According to the current state of the art, fibre optic cables, which are insensitive to electromagnetic interference, permit flow rates of the order of 10Gbits/second.[12] Present day cables contain several fibres (from a few dozen to a few hundred). Thanks to DSL technology, it is normal to achieve flow rates of up to four megabits a second without having to modify the conventional twisted pair telephone wire and with equipment costing less than a hundred euros. This means it will become technically possible for television to be distributed via the internet rather than satellite or a dedicated coaxial cable. Experiments along these lines are under way in a number of countries. This presents a new challenge. At the moment, satellite and cable distribution technically do not, or hardly, enable the broadcaster to know what programmes the consumer is watching – all the signals arrive at the terminal device of the subscriber, who chooses what to watch. In the case of internet television, it will be possible to find out what each individual is watching and even insert advertising targeted at him or her at precisely chosen moments.

[10] As regards a more comprehensive description of the new technological landscape and its evolution, see Poullet and Dinant, *Information Self-Determination in the Internet Era*, unnumbered note on p. 60, above.

[11] See below n. 32 and following text.

[12] This refers to the equipment currently installed. Prototypes enable much faster speeds to be achieved.

Processing power has increased in correlation to the power and capacity of computer components. In 1987, a typical PC had an 8 MHz processor with 640 KB of random access memory and a hard disk of 20 megabytes. In 2004, a computer typically on sale in supermarkets had a 2.4 GHz processor (3,000 times more), 256 MB of RAM (400 times more) and a hard disk with a capacity of 60 GB (3,000 times more). Moreover, at equivalent speed, modern processors are significantly more powerful than their predecessors. There is an increasing tendency for computers to contain a greater number of processors, some of which play a more specialised role controlling a specific task (for example, display or the transmission and reception of signals on the network).[13] Certain processes, which used to be impossible, are now becoming perfectly feasible. The sampling and digitisation of a voice or an image can now be done in real time, with the result being of a quality very close to the original. Thus, it will become more and more possible and less expensive to record the lives of all individuals on the planet.[14]

The third characteristic of the internet is the open nature of the network and the associated range of available applications. Openness, in the sense that anyone can log on anywhere at any time, raises questions about the confidentiality of the messages circulating on a network that is not quite secure.[15] Openness also means that messages placed on the internet, say one's curriculum vitae or publications listed on it or even one's photograph, can be retrieved thanks to the power of a search engine and subsequently used for a different purpose – a purpose that may be uncontemplated at the time the information was put on the internet originally. Additionally, in travelling from one point to another on the internet, one can 'jump' endlessly from one site to the next producing a multitude of traces in different places in the process.

The global dimension of the network and the multitude of transborder movements give rise to unease regarding the privacy implications

[13] E.g. ASIC chips (or Application Specific Integrated Circuits) which are processors specially designed for a specific task (e.g. the digitisation of an analogue signal, encryption or decryption). Typically, an ASIC chip will run approximately one hundred times faster than a non-application-specific processor to carry out a particular task.

[14] Just one example: The Belgian National Register, which contains the demographic details of all Belgians from their birth to their death as well as their occupations, marriages and death and successive addresses (not counting the data on foreign residents in Belgium) would today easily fit onto a DAT cassette the size of a large box of matches or on a few DVDs. It could be transmitted in its entirety by fibre optic cable in less than a minute.

[15] The anticipated generalised use of cryptic systems certainly would be a big step forward. The issue is addressed in Directive 2002/58/EC of 12 July 2002, above n. 2.

of the internet. The various data protection systems currently in place are extremely disparate. There may even be no protection at all in some countries through which data travels or on whose sites they end up. Another concern is raised by the case of Echelon, an integrated global surveillance network used to intercept messages transmitted by satellite owned by certain state information services including the United States, United Kingdom, Canada, Australia and New Zealand.[16] The idea that messages, including those in the national interest, can be captured by foreign powers as they are being transmitted by satellite demonstrates the limits of national sovereignty and the relative failure of national privacy protection systems. This is a particular problem in Europe.

Add to these features the opaque nature of the internet. The recent literature shows the range of applications said to have been engendered by means of cookies,[17] by the so-called 'global unique identifiers',[18] and through invisible hyperlinks.[19] This hidden face of the internet allows for picking and choosing between internet users. For instance, it facilitates various techniques of cyber-marketing, the efficacy of which becomes more remarkable by the day. These techniques permit such things as targeted advertising, differential pricing, even selective denial of access to websites by users deemed insufficiently financially worthwhile. The opaque nature of the internet further allows for the multiplication of actors, at times making it hard to identify readily their location, intervention or relationship between one another. Who knows about the precise role of internet access providers, of gateways and the link between these and the sites they list or refer to? Who knows about the role of search engines, not to mention browsers that pass on information to not easily identifiable actors, often without the knowledge of the users?

It follows that the internet entails major serious risks for the privacy of its users. This realisation forces a reconsideration of legislative provisions

[16] See European Parliament, *Report*, above n. 4.

[17] Cookies are pieces of information generated by a web server and stored in the user's computer when a web site is accessed. They allow web servers to recognise the user each time the site is returned to. In most cases, not only does the storage of personal information into a cookie go unnoticed, so does access to it: see, generally, Viktor Mayer-Schönberger, 'The Internet and Privacy Legislation: Cookies for a Treat?' (1997) 1 *West Virginia Journal of Law and Technology* 1.1.

[18] On this system developed by Microsoft, as well as on PSN (Personal Serial Number) developed by Intel, see J. Marc Dinant, 'Law and Technology Convergence in the Data Protection Field' in Ian Walden and Julia Hörnle (eds.), *E-Commerce Law and Practice in Europe* (Cambridge: Woodhead, 2002), chap. 8.2.

[19] See, in particular, J. Marc Dinant, *Les traitements invisibles sur Internet*, available at http://www.droit.fundp.ac.be/crid.

and the principles upon which these are based. That will be the focus of the next discussion. The adoption of new rights will be addressed under a separate heading. The chapter will end with a look at how the market itself may provide more effective privacy protection.

Towards a reconsideration of the legal rules and principles on privacy protection

The invasion of everyday life by the internet is a recent phenomenon. The European Directives and their national implementation measures could not take into account this development and its associated risks. In determining how the principles and concepts of the Directives on privacy protection will be applied, we first need to interpret the existing rules. Only where the existing law fails to provide a satisfactory solution is it necessary to resort to more proactive methods of rule creation. A comprehensive examination of the privacy Directives is beyond the scope of this chapter. The discussion below is limited to analysing certain relevant legislative provisions, reflecting on the conditions for legitimate use (in particular the notion of consent), and ending with some consideration of cross-border flows of information.

Definition of 'personal data'

One of the more controversial issues is the extension of the concept of personal data to information created by cookies. Recent literature on this issue starts from the proposition that cookies put information onto the hard drive of the user's computer so as to allow identification, not of the user personally but of his or her computer.[20] Each time the user reconnects to the relevant site, recognition occurs. According to Article 2(a) of the 1995 Data Protection Directive, personal data is 'any information relating to an identified or identifiable natural person' (the 'data subject'). Does this mean that information collated by cookies is beyond the scope of the privacy protection laws simply because only a computer is being identified? The 1995 Directive treats as identifiable a person who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to his or her physical, physiological,

[20] See, in particular, Marie-Hélène Boulanger and Cécile de Terwangne, 'Internet et le respect de la vie privée' in *L'Internet Face au Droit* (no. 12, Namur: Centre de Recherche Informatique et Droit, 1997).

mental, economic, cultural or social identity. Pursuant to preamble 26 of the 1995 Directive, for the purpose of determining the notion of 'identifiability' the totality of the means 'likely reasonably to be used', either by the controller or by any other person, should be taken into account. Does this assessment occur *in abstracto* or *in concreto*? The terms of the Directive do not answer this question. Yet, it is a relevant question because companies working with cookies generally claim that they do not engage in research to identify the physical person.

This concept of 'identity' applied to cookies but applying it beyond – to a global unique identifier or a simple IP address[21] – remains ambiguous. And this ambiguity remains in the way it was interpreted by various European countries when they transposed the 1995 Directive into their respective national legislation. I shall take as examples the transpositions carried out by Belgium, the United Kingdom and Sweden.

Belgian law defines as personal data:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[22]

This is a carbon copy of the text of the directive.

The scope of the British legislation is narrow because it states that:

> personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.[23]

The Freudian slip may be noted. It could be said that data relating to an individual are not personal data if the data controller cannot identify the person concerned. However, in this situation there are no personal data,

[21] Or, as regards the future IPv6, see Article 29 Working Party, *Opinion 2/2002 on the use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of IPv6*, 10750/02/EN/final, WP 58, 30 May 2002.

[22] Law of 8 December 1992, as modified by the Law of 11 December 1998. A consolidated version of this law is available at the web site of the Belgian Privacy Commission (which can also be translated as the Data Protection Authority or the Commission for the Protection of Personal Privacy), http://www.privacy.fgov.be.

[23] Data Protection Act 1998, s. 1. As regards the narrow interpretation of the concept under case law, see *Durant* v. *Financial Services Authority* [2004] FSR 28.

there is no processing of data and, consequently, there could be no 'data controller'.[24]

In Sweden, the Personal Data Act 1998 defines personal data as '(a)ll kinds of information that directly or indirectly may be referable to a natural person who is alive'. Surprisingly, no mention is made here of the notion of identity.[25] It could be thought that the Swedish law (which was intended to transpose the 1995 Directive) considers that information cannot be attributed to a natural living person without him or her being identified. On the internet, it is possible to imagine a customer who cannot be identified at all (for example, by using an anonymising site) and is assigned a number of non-identifying cookies attesting to his or her homosexuality and interest in AIDS treatments. In the strict framework of the 1995 Directive, the law would not apply to these two cookies because they do not relate to an identifiable person. However, the website (for example, one offering life assurance quotations online) that receives this visitor and his or her cookies could conclude, rightly or wrongly, that he or she has a relationship with a homosexual who probably has AIDS. The Swedish law, on the other hand, could become applicable if the feature 'homosexual, probably with AIDS' is *attributable*, at the moment of the connection, to a living natural person, even if he or she remains unidentifiable.

Saying that, we have to concede that considering an item of data (such as a cookie, the IP address or a global unique identifier) as 'personal data' will lead to the application of the provisions of the 1995 Data Protection

[24] Here, the drafters have disregarded the precision introduced by Recital 26 of Directive 95/46/EC of 24 October 1995, above n. 1. This leads to collateral damage: imagine the manager of a supermarket simply noting the registration numbers and types of the vehicles in the car park as well as their arrival and departure dates and times. Generally, it is not very likely that a supermarket manager will be able to go so far as to identify the person concerned simply from the registration number in his or her possession. This type of recording system would therefore not be covered by the UK's Data Protection Act 1998. There are no personal data, so there is no data processing let alone a 'data controller'. This system can be extended, refined and consolidated at the national level and this would provide a system that enables vehicles to be tracked via the car parks throughout the country. It is thus easy to imagine such a system on the internet in a data paradise, with anyone whatsoever being able to piece together the itinerary or even timetable of his or her neighbour, boss, lover or spouse.

[25] On this ambiguous concept applied to the genetic data, see Gaia Bernstein, 'Information Technologies and Identity' [2005] 1 *Computer Law Review International* (formerly *Computer und Recht International*) 1–7.

Directive 95/46/EC and, accordingly, the obligation to process this data,[26] even though it would not normally have been processed. In addition, the application of the provisions, such as the obligation to inform the person concerned, could prove impossible without identifying him or her. But in another sense, we have to underline that not treating the IP address and the global unique identifier as items of personal data would pose a problem because of the risks that subsequent use of these data represent in terms of profiling the individual and, indeed, the possibility of contacting him or her. There is evidence that, with the combination of web traffic surveillance tools, it is easy to identify the behaviour of a machine and, behind the machine, that of its user. In this way the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the 'identity' of the individual – that is, his or her name and address – it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her identity in a traditional sense.

Categories of data

The scope of application of the Privacy and Electronic Communications Directive 2002 is considerably wider than the 1997 Directive it replaces. Whereas the 1997 Directive applied to telecommunications services and networks, the 2002 Directive covers all services and networks in the electronic communication sector, at least where these are open to the general public. The idea is to bring within the same regulatory framework all services and networks whose main object is the transmission and routing of signals regardless of the technology used, including provision of access to the internet as well as 'remailing' services. This extended coverage of European law is important in that it sets up a separate regime for data processing that occurs within these networks, in particular involving data about traffic and so-called location data. The latter is a new concept. The former already featured in the 1997 Directive, but the 2002 Directive now provides a definition of both concepts.

[26] If only to enable rights of access, and so forth.

Under the 2002 Directive, the concept of traffic data embodies 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.[27] This includes the address label of an internet transmission – either that of the sender or the receiver – the length of the communication and also the protocols used. Pursuant to Article 6 of the 2002 Directive, this type of data must be 'erased or made anonymous when it is no longer needed for the purpose of the transmission of the communication'. Three exceptions are allowed: where the data is needed for billing purposes; where consent, which might be revoked at any moment, is given for the purpose of marketing electronic communication services or the provision of value added services; and where the data is required by proper authorities for settling disputes, in particular about interconnection or billing.[28]

Location data are defined as 'any data processed in an electronic telecommunications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.[29] Examples are precision location data attached to the possession and use of mobile terminal equipment, the offer of value added services by some operators, and services that rely on localisation being possible such as, for example, guidance services for drivers. The 2002 Directive prohibits the processing of the above data without the revocable consent of the user or subscriber to the service, or beyond the extent or duration necessary for such service.[30] Users or subscribers must be given the possibility to withdraw their consent at any time.

An analysis of the European provisions on traffic and location data reveals important deviations from the principles on the legitimacy of data processing as signalled by Article 6 of the 1995 Data Protection Directive. Under the 1995 Directive interests may be weighed in deciding whether data processing is permitted.[31] Under the 2002 Directive, the primary if not sole basis for the processing of traffic and location data is when it is duly legitimated by the service offered or the prior consent of the persons

[27] Directive 2002/58/EC of 12 July 2002, above n. 2, Art. 2(b). On the European regulation of traffic data, see Brigitte Zammit, 'Traffic Data Retention under EC Law' (2005) 11(1) *Computer and Telecommunications Law Review* 17.

[28] Directive 2002/58/EC of 12 July 2002, above n. 2, Art. 6(b) and (c).

[29] Ibid. Art. 2(c). [30] Ibid. Art. 9(b).

[31] Directive 95/46/EC of 24 October 1995, above n. 1, Art. 7(f), discussed below n. 36 and accompanying text.

concerned.[32] This restriction, when applied in the context of internet use, can be striking.[33]

Legitimacy of the processing

Consent as a basis for the legitimacy of processing

The scope for applying the consent requirement in the context of the internet is extremely wide. For instance, it makes employer monitoring of employee internet use, including the transfer from site to site via hyperlinks, conditional upon the user's consent.[34] Two justifications for this omnipresent consent requirement come to mind.[35] The first has to do with the risks associated with the possible multitude of processing operations. It justifies adopting a restrictive approach to the grounds for legitimate data processing. In particular, it calls for close scrutiny of

[32] Traffic data retention for law enforcement purposes or for the network's own security purposes is not developed. On that point, see the discussion around the presently discussed *Draft Framework Decision on the Retention of Data*, above n. 7. On the draft, EPIC comments and further material are available at http://www.epic.org./privacy/intl/data_retention.html.

[33] Thus, e.g., Art. 314, 2 of the Belgian Penal Code prohibits anyone from receiving, intercepting, or listening to private communications or telecommunications, unless all parties concerned agree. The 17th Chamber of the Criminal Court of Paris had occasion to enforce this principle when it ruled against a research laboratory that expelled a student upon becoming aware of personal email use: Corr Paris, 2 November 2000. The text of the decision can be found at http://www.droit-technologie.org.

[34] The Belgian Privacy Commission has issued a qualified recommendation in this regard: Commission de la Protection de la Vie Privée, *Avis no. 10/2000 d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail*, 3 April 2000. Recommendation 10/2000 acknowledges a certain legitimacy of employer control over the use of company equipment. For the Commission the question is one of proportionality between the control mechanisms used and the risks run by the employer. Thus, checking the contents of employee email is not necessarily legitimate where the installation of filters can equally reduce illegitimate use. As regards the German situation, the same principles are available; see, on that point, Jan-Malte Niemann, 'Monitoring Internet and Email Usage – Germany – Surfing into Unemployment? Private Internet Use and Emailing Under German Labour Law' (2002) 18(2) *Computer Law and Security Report* 114. It would seem that in North America employees do not enjoy a similar 'reasonable expectation' that their privacy is to be protected in the use of the email system: see, H. L. Rasky, 'Can an Employer search the Contents of his Employees' E-mail?' (1998) 20 *Advocates' Quarterly* 221.

[35] On the consent requirement we might take into account the warnings by Léonard against an overly wide application; see Thierry Léonard, 'E-commerce et protection des données à caractère personnel: quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet', February 2000, available at http://www.droit.fundp.ac.be/Textes/Leonard1.pdf.

Article 7(f) of the 1995 Directive as that provision permits data processing following a weighing of the various interests at stake.[36] This weighing of interests is difficult to carry out in practice. It presupposes that the individual concerned is able to know all the processed data and able to ensure that his or her interests are taken into account. At times this can be most problematic given the global nature of the network. The second justification relates to the interactive nature of the network, in that this allows for consent to be fully possible. In effect, it is the person concerned who, by using his or her equipment, is the author of the data created. Why not let that person decide whether he or she wishes to receive cookies, identify himself or herself, have his or her data transmitted to a third party, receive advertising messages, and so forth? Consent allows the consumer to decide whether or not he or she wishes to part, possibly in exchange for hard currency, with his or her personal data.

The requirement that there be a legitimate purpose involves considering the question of consent as the basis for the legitimacy of certain processing operations carried out in connection with the use of internet services by the data subject. As we know, even if Article 5 limits itself to mentioning the general principle of legitimacy, the issue of consent is mentioned by the data protection authorities, by the European Directive in Article 5.1, and by legal writers as the primary basis for the legitimacy of a processing operation. Since modern networks are interactive, consent can more easily be claimed to be the basis for the legitimacy of data processing and be preferred to other more traditional bases such as a balance of interests. The ease with which the file controller can obtain the data subject's consent explains why some countries' laws do not hesitate now to demand that consent be given in order to legitimise certain processing operations, like the 2002 Directive on the processing of traffic and location data.[37]

This consideration now leads some to believe that consent may be enough to legitimise processing. It should be remembered in this connection that the development by the World Wide Web Consortium (W3C) of

[36] Directive 95/46/EC of 24 October 1995, above n. 1, Art. 7(f) provides that data processing may be permitted if 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which requires protection under Article 1(1)'.

[37] Mention should also be made of the opt-in system chosen to resolve the question of sending unsolicited mail. Other arguments in favour of the ability to opt in are the intrusive character of the mail that directly penetrates the data subject's home, the ease with which such messages can be sent and the absence of any costs for the sender.

the Platform for Privacy Preferences (P3P)[38] was also based on the possibility for web surfers to negotiate with service providers who failed to respond to their privacy preferences and reach an agreement that would serve as a legitimate basis for the planned processing operation. Even if no broad use has ever been made of this possibility of holding negotiations, especially through electronic agents, P3P remains an indication of the industry's willingness to provide itself with the means of negotiating with the data subject the use that might be made of his or her data. The protection of privacy could thus to some extent be negotiated.[39]

Nevertheless consent does not appear to us to be a sufficient basis for legitimacy. We think that, in certain cases, even the legitimacy of processing that is backed by a person's specific, informed and freely given consent may be called into question. There are three reasons that support this view. First, even consent that has been obtained by fair means cannot legitimise certain processing that is contrary to human dignity or to other key values that an individual cannot relinquish. Secondly, consumers must be protected against practices that involve their consent being solicited in exchange for economic advantages.[40] Finally, the question of the protection of privacy is not just a private matter, but brings social considerations into play and calls for the possibility of intervention and supervision by authorities.[41]

The consent of minors to the processing of personal data concerning them poses some tricky problems. The consent must come from a person legally capable of giving it. The consent given by a minor is on no account sufficient without parental authorisation, but this does not prevent minors having to be consulted – provided that they understand – or even requiring not only parental authorisation but also the minor's own autonomously

[38] See Article 29 Working Party, *Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, XV D/5032/98, WP 11, 16 June 1998. See also, on this protocol, Jason Catlett, *Open Letter 9/13 to P3P Developers*, 13 September 1999, available at http://www.junkbusters.com/standards.html.

[39] On the technology-based contractualisation of the processing of data, see Paul M. Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace, Filters, Privacy Control and Fair Information Practices' (2000) *Wisconsin Law Review* 749; Marc Rotenberg, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' (2001) *Stanford Technology Law Review* 1.

[40] As noted by Léonard, 'E-commerce et protection', above n. 35, the rules in general contract theory as regards defects in the consent, especially the rules on taking unfair advantage, must be complied with.

[41] Cf. in this connection the thoughts put forward by Schwartz, 'Beyond Lessig's Code for Internet Privacy', above n. 39.

expressed consent. Recently, the development of interactive internet services has given these principles a particular topicality. Children are a preferred target for all kinds of internet 'vendors' and several methods of gathering information are used to induce them to provide personal information, such as competitions, membership forms, and so forth. It thus appears necessary to check parental consent to the provision of such information. The US Children's Online Privacy Protection Act (COPPA) of 1998 requires that the provider of services that gather information from minors be subject to the principle of 'verifiable parental consent', which is defined as:

> any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.[42]

Recently, the Belgian Privacy Commission issued a more guarded opinion on the same subject, stressing the child's autonomy and underlining the limits to it:

> The Commission is of the opinion that parental consent does not have to be systematically required when data relating to a minor are processed on the internet. It thus emphasises that parental consent should not be a mechanism permitting a parent to override the child's decision unless there is a serious risk that the child will not correctly appreciate the consequences of its decision or that its natural naivety will be exploited. The Commission therefore stresses in this document the necessity to obtain parental consent in specific circumstances, especially when the child has not reached the age of discernment, when sensitive data are gathered, when the aim pursued is not in the minor's direct interests (marketing, transmission of the data to third parties) or when the data are to be made public (dissemination of information at a discussion forum or at a school's website).[43]

[42] Children's Online Privacy Protection Act 1998 (US) s. 1302(9). The text of the law is available at the Federal Trade Commission's website http://www.ftc.gov/ogc/coppa1.htm. The law provides for some exceptions to this requirement.

[43] Belgian Privacy Commission, *Opinion on the Protection of the Privacy of Minors on the Internet*, Avis no. 38/2002, 16 September 2002. Available at the Commission's website: http://www.privacy.fgov.be.

Incompatible processing

The principle of the 'compatibility' of purposes requires that, in the case of subsequent processing, these operations must not clash with the reasonable expectations of the person concerned. The acceleration of technological progress, the infinite number of new processing opportunities offered by the software, and the data available on the network warrant giving some attention to the question of subsequent processing and its compatibility with the initial aims of data recording. More and more data are stored in huge data warehouses in order to be reused in the future for new applications, taking into account new technological possibilities or scientific progress.

For example, Radio Frequency Identifier or RFID chips, which were originally designed by consumer goods manufacturers as a means of preventing theft in big department stores, have become a powerful tool for analysing the behaviour of consumers, their profiles, and so forth. If scientific authors make their curriculum vitae and publications available for the purpose of making their work known, this may serve to classify them politically or in terms of their analyses. The publication of court judgments in huge databases has an academic objective and helps to make the law known. However, the possibility of running a search of the names of the parties or the type of case may enable blacklists to be drawn up (for example, a list of employees who have brought an action against or been dismissed by their employers).

The proportionality of the data

Some comments about the contents of data processing are in order. The European Directive asserts clearly that the data processed must be relevant, proportionate and not excessive as regards the legitimate purposes pursued by the data controller. The possibilities offered by the internet in collecting data, especially given the interactive nature of the net, explain the discrepancy between the sheer volume of data retained or handled and the legitimate purpose pursued by those responsible for processing the data. An example is the data processing that occurs in the context of employee surveillance by companies.[44] An illustration may be given from

[44] Pursuant to this principle, what the Belgian Privacy Commission questions is not so much the legitimacy of the data handling but rather the possible disproportionate size of their contents. To control an employee's activities does not necessitate the detailed collection

a 1998 OECD study on electronic commerce sites.[45] The study shows that for nearly two thirds of sites the information asked for – via subscription lists, feedback forms, and especially questionnaires – is optional. Among this optional information typically feature the individual's email address, telephone number, age, gender, occupation, certain preferences and personal habits. At times the answers to these optional questions allowed visitors to gain award points or enter a competition.

Trans-border data flows

The internet and over 60 percent of sites continue to be North American: any European traffic on the internet takes place on non-European webs. This explains the concern of the public authorities about cross-border movement of data. The provisions of Articles 25ff of the 1995 Directive hold that the transfer to a non-EU country of personal data that is the object of processing after their transfer cannot occur unless the country in question provides assurance about an adequate level of data protection. Exceptions to this principle exist, either in certain specific instances of legitimate movement, or where sufficient contractual safeguards are in place. Without claiming to be exhaustive, two questions arise. A first question concerns the scope of application of the provisions. A second question concerns the standards adopted by foreign countries for the provision of adequate data protection safeguards.

As to the first, Article 4 of the 1995 Directive provides that Member States should apply their laws extraterritorially where 'for the purposes of processing personal data [the controller] makes use of equipment . . . situated on the territory of the said Member State, unless the equipment is used only for purposes of transit through the territory of the Community'. Many academic scholars concur with Boulanger and Terwangne who argue that the Directive applies to narrowly defined instances of passive trans-border movements; that is, those that occur without the knowledge of the person concerned and that involve the use from a distance

of all terminal activity by that employee. Rather, the collection of general data may suffice such as, e.g., time spent on the computer, type of services used. See, on the opinion of the Belgian Privacy Commission, Stanislas Van Wassenhove, Michael De Leersnyder and Gael Chuffart, *Nouvelles technologies et impact sur le droit du travail* (Kortrijk-Heule: UGA, 2003) pp. 81–97.

[45] OCDE, *Pratiques relatives à la mise en oeuvre sur les réseaux mondiaux des lignes directrices de l'OCDE sur la vie privée*, DSTI/ICC/REG (98) 6, Paris, 18 and 19 May 1998.

of the user's equipment to collect data.[46] Also covered is data processed by cookies or other means such as the global unique identifier as well as cases of 'web spoofing' where data collection occurs via a mirror site based in a European country.[47] An analogous case is the case of Yahoo which gained some adverse publicity when proceedings were launched by *La Ligue Contre le Racisme et l' Antisémitisme* objecting that anti-Semitic material could be accessed from one of its websites. It was shown that the site Yahoo.fr simply served as a collection instrument without local handling of the data in France. The French court ruled against the Yahoo company.[48]

Some commentators have raised doubts about the applicability of Articles 25ff of the 1995 Directive whenever the user is in direct contact with a foreign site. Modifications have been made in some of the implementing national laws. For instance, Article 3bis of the Belgian law limits its reach to instances where the processing occurs in the context of real and effective activities of a business based in Belgium or where the processing is done by means, whether or not automated, in Belgium. The first scenario is said not to cover instances where the data generated by a site visit do not constitute handling or processing, at least not in Europe. However, this interpretation seems to go against the 1995 Directive, which the Belgian legislation was meant to implement. The Directive gives the Member States specific powers in matters of trans-border movements, whether or not the exported data have been the subject of processing in Europe. And Article 4 of the 1995 Directive, upon which Article 3bis of the Belgian legislation is based, does not seek to determine the substantive scope of application of the Directive; rather it sets out to determine the applicable national law as regards data processing.

[46] Marie-Hélène Boulanger and Cécile de Terwangne, 'Internet et le respect de la vie privée' in Etienne Montero (ed.), *L'internet face au droit*, Cahier du CRID no. 12 (Namur: Story-Scientia, 1997).

[47] In that sense, see Article 29 Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Websites*, 5035/01/EN/Final, WP 56, 30 May 2002.

[48] The case concerned the complaint by several French groups against the Yahoo company for harbouring Nazi objects on its sites. The president of the French court of first instance at two occasions (on 22 May and again on 20 November 2000) ordered Yahoo to take all necessary steps to discourage and prevent the auctioning and sale of Nazi memorabilia. The text of the decisions of the Tribunal de Grande Instance, as well as some commentaries, is available at www.juriscom.net/txt/jurisfr/cti/ tgiparis20001120.htm. For parallel action taken in the United States by Yahoo, see *Yahoo!, Inc.* v. *La Ligue Contre Le Racisme et L'Antisémitisme*, 379 F 3d 1120 (9th Cir. 2004) and 399 F 3d 1010 (9th Cir. 2005).

In the *Lindqvist* case,[49] the European Court of Justice had to solve the following question. Does the insertion on a web page located on a host server located in Europe but accessible from foreign countries constitute a trans-border data flow in the sense of Articles 25ff? In a highly criticised decision,[50] the court considered that the author of the website pages containing personal data had not transferred the data to foreign countries insofar as the author only furnished the pages to a national hosting provider, even if the purpose was to render these web pages accessible throughout the world. The main reason invoked by the court was its concern of seeing all postings on internet web pages automatically subject to the restrictions imposed by Articles 25ff.

If it is correct that Articles 25ff of the 1995 Directive apply to most trans-border movements via the internet, a determination of the adequate nature of the safeguards offered by the foreign country must be made. The EC Commission examined the Safe Harbour Principles drafted by the US Department of Commerce, to which American companies are expected to subscribe,[51] and concluded that they satisfy the adequate safeguard requirement of the Directive – although this has not been the case for all countries whose privacy laws have been reviewed by the Commission.[52] Furthermore the European Commission has proposed to companies alternative models offering 'appropriate safeguards' for the transfer

[49] *Lindqvist* [2003] ECR I-12971; [2004] QB 1014 (Case C-101/01).

[50] See, in particular, Cécile de Terwangne, 'Affaire *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles' (2004) 19 *Revue du Droit des Technologies de l'Information* 67 at 88ff.

[51] The text of the safe harbour principles may be found on the internet site of the US Department of Commerce at http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm. In brief, six basic principles form the core of the 'Safe Harbor Principles'. They relate to information on the person concerned; restrictions on transfer; security; integrity of the data; access by the person concerned and effectiveness of the principles themselves. As for the latter, there exist mechanisms to appeal to independent private authorities and action may be taken by the Federal Trade Commission in instances of misrepresentation. On the implementation of the Safe Harbour Principles and its assessment, see the CRID study prepared for the EU Commission (Internal Market DG): Jan Dhont, María Verónica Pérez-Asinari and Yves Poullet (with the assistance of Joel R. Reidenberg and Lee A. Bygrave), *Safe Harbour Implementation Study* (Namur: CRID, 2004); available from http://europa.eu.int/comm/justice_home/fsj/privacy/.

[52] Other decisions have been taken by the Commission under the Article 25.6 basis, notably vis-à-vis Argentina, Switzerland, Canada. The legislative system proposed by Australia as regards the private sector on the contrary has been judged as inadequate by the Commission insofar as notably too broad exceptions have been allowed under the Australian Act for small enterprises, employees' data and the absence of protection for foreigners' data (See: Article 29 Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN, WP 40, 26 January 2001).

of personal data.[53] So the Commission adopted in 2001 two decisions on standard contractual clauses for the transfer of the data outside the European Economic area – for the transfer of personal data to controllers and processors established abroad[54] – and more recently has issued an opinion about 'binding corporate rules'; that is, self-regulatory data protection safeguards which are put in place by multinational companies on the basis of their own needs and culture and offer more flexibility than contractual clauses.[55]

Towards the recognition of new rights

Those features that are most characteristic of the electronic communications service environment – growing presence and multifunctionality of electronic communications networks and terminals, their interactivity, the international character of networks, services and equipment producers and the absence of transparency in terminal and network functioning – all increase the risk of infringing individual liberties and human dignity.

To counter these risks, certain new principles must be established if data subjects are to be better protected and have more control over their environment. Such control is essential if those concerned are to exercise effective responsibility for their own protection and be better equipped to exercise proper informational self-determination. This is a first attempt to outline such principles. It is based on a range of material and we have tried to structure it around five main principles, since at this stage we prefer not to speak of new 'rights' for data subjects. Their content and extension should be discussed by the Council of Europe Consultative Committee on Convention no. 108, and could then, if appropriate, form the basis for recommendations and other ad hoc measures to give them greater force.

[53] The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26(4) of Directive 95/46/EC that certain standard contractual clauses offer sufficient safeguards as required by Article 26(2), that is, they provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

[54] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document no. C(2001) 1539) 2001, *OJ*, L 181, 4 July 2001, 19; and Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (notified under document no. C(2001) 4540) 2002, *OJ*, L 006, 10 January 2002, 52.

[55] Article 29 Working Party, *Working Document on Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, MARKT/11639/02/EN, WP 74, 3 June 2003.

The principle of encryption and reversible anonymity

The encryption of messages offers protection against access to the content of communications. The quality varies, as do encryption and de-encryption techniques. Encryption software for installation on internet users' computers (S/MIME or Open PGP protocols) is now available at a reasonable price. Given its ambiguity, the notion of anonymity should perhaps be clarified, and possibly replaced by other terms such as 'pseudonymity' or 'non-identifiability'. What is sought is often not absolute anonymity but rather the functional non-identifiability of the author of a message vis-à-vis certain persons.[56] There are many non-binding documents advocating citizens' 'right' to anonymity when using new technological services.[57] Recommendation R (99) 5 of the Council of Europe's Committee of Ministers states that 'anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy',[58] hence the importance of privacy enhancing techniques already available on the market.

Those using modern communication techniques must be able to remain unidentifiable by service providers and other third parties during the transmission of the message and by the recipient or recipients of the message, and should have free or reasonably priced access to the means of exercising this option.[59] The availability of readily affordable encryption and anonymisation tools and services is a necessary condition for computer users exercising personal responsibility.

[56] See Jan Grijpink and Corien Prins, 'Digital Anonymity on the Internet: New Rules for Anonymous Electronic Transactions?' (2001) 17 *Computer Law and Security Report* 379.

[57] See, in particular, Stefano Rodota, 'Beyond the EU Directive: Directions for the Future' in Yves Poullet, Cécile de Terwangne and Paul Turner (eds.), *Privacy: New Risks and Opportunities*, Cahier du CRID no. 13 (Antwerpen: Kluwer, 1997) p. 211ff.

[58] Council of Europe, Committee of Ministers, *Guidelines for the Protection of Individuals with regard to the Collection and Processing of Personal Data on Information Highways*, Recommendation no. R (99) 5, 23 February 1999. See also Article 29 Working Party, *Recommendation 3/97: Anonymity on the Internet*, DG MARKT D/5022/97, WP 6, 3 December 1997; and the opinion of the Belgian Privacy Commission on electronic commerce: *Avis no. 34/2000 relatif à la protection de la vie privée dans le cadre du commerce électronique*, 22 November 2000 (available at http://www.privacy.fgov.be) which points out that there are ways of authenticating the senders of messages without necessarily requiring them to identify themselves.

[59] See the recommendation of the French Commission for Privacy that access to commercial sites should always be possible without prior identification: Marie Georges, 'Relevons les défis de la protection des données à caractère personnel: l'Internet et la CNIL' in P. Lemoire (ed.), *Commerce électronique- Marketing et vie privée* (Paris: LaSer, 1999), pp. 71–2.

The anonymity or 'functional non-identifiability' required, however, is not absolute. Citizens' right to anonymity has to be set against the higher interests of the state, which may impose restrictions if these are necessary 'to safeguard national security, defence, public security, [and for] the prevention, investigation, detection and prosecution of criminal offences'.[60] Striking a balance between the legitimate monitoring of offences and data protection may be possible through the use of 'pseudo identities', which are allocated to individuals by specialist service providers who may be required to reveal a user's real identity, but only in circumstances and following procedures clearly laid down in law.

Other approaches might include the enforced regulation of terminal equipment, to prevent browser chattering, permit the creation of ephemeral addresses and differentiation of address data according to which third parties will have access to the traffic or localisation data, and the disappearance of global unique identifiers by the introduction of uniform address protocols.

Finally, the status of 'anonymisers', on which those who use them place great reliance, should be regulated to offer those concerned certain safeguards regarding the standard of service they provide while ensuring that the state retains the technical means of accessing telecommunications in legally defined circumstances.[61]

The principle of reciprocal benefits

This principle would make it a statutory obligation, wherever possible, for those who use new technologies to develop their professional activities to accept certain additional requirements to re-establish the traditional balance between the parties concerned. The justification is simple – if technology increases the capacity to accumulate, process and communicate information on others and facilitates transactions and administrative operations, it is essential that it should also be configured and used to ensure that data subjects, whether as citizens or consumers, enjoy a proportionate benefit from these advances.

Several recent provisions have drawn on the proportionality requirement to oblige those who use technologies to make them available for users

[60] Directive 2002/58/EC of 12 July 2002, above n. 2, Art. 15.

[61] Requirements could be laid down for the services provided and concerning confidentiality, as is proposed for electronic signatures. Official approval of an anonymiser would indicate that the requirements were being observed. Such official approval might be voluntary rather than obligatory, as in the case of quality labels.

to enforce their interests and rights. So Article 5.3 of the 2002 Directive on privacy and electronic communications even includes the requirement that 'the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information . . . and is offered the right to refuse such processing'. Subscribers' right, under Article 8.1, 'via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis . . . and on a per-line basis' is another potentially valuable approach if the notion of 'calling line' is extended to various internet applications, such as web services and email.[62] This implies a related obligation for the service provider to offer users the options of refusing to accept unidentified calls or preventing their identification.[63]

Legislation of the freedom of information variety introduces a similar right to transparency vis-à-vis government by adding further information that the latter is obliged to supply. A welcome development in the UK is the recent introduction of a public service guarantee for data handling.[64] A Swedish commission has recently recommended legislation that would entitle citizens to monitor their cases electronically from start to finish, including their archiving, and oblige the authorities to adopt a good public access structure, to make it easier for individuals to identify and locate specific documents.[65] There is even draft legislation that would make it possible to link any official documents on which decisions were based to other documents about the case. In other words, a public service that has become more efficient thanks to new technology must also be more transparent and accessible to citizens. Citizens' right of access extends beyond the documents directly concerning them to include the regulations on which a decision was based.

[62] Note the link between these provisions and the anonymity principle.

[63] See Art. 8.2 and 8.3 of Directive 2002/58/EC of 12 July 2002, above n. 2.

[64] The UK Department for Constitutional Affairs has released a public service guarantee for data handling which is available for implementation in public bodies. It sets out people's rights about how their personal data is handled by public authorities and the standards they can expect public organisations to adhere to, see http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2.

[65] Peter Seipel, 'Information System Quality as a Legal Concern' in Urs Gasser (ed.), *Information Quality Regulation: Foundations, Perspectives, Applications* (Baden-Baden: Nomos, 2004) p. 248. See also the Swedish ICT Commission report: Peter Seipel (ed.), *Law and Information Technology: Swedish Views*, Swedish Government Official Reports, SOU 2002: 112.

It is even possible to imagine that certain of the rights associated with data protection – such as the right to information, the rights of access and rectification, and the right of appeal – might soon be enforceable electronically. Many applications could be proposed, including the five suggestions that follow.

It should be possible to apply data subjects' right to information at any time through a simple click (or more generally a simple electronic and immediate action) offering access to a privacy policy, which should be as detailed and complete as the greatly reduced cost of electronic dissemination allows. Such a step must be anonymous as far as the page server is concerned, to avoid any risk of creating files on 'privacy concerned users'. In addition, in the case of sites that have been awarded quality labels, it should be obligatory to provide a hyperlink from the label symbol to the site of the body that awarded the label. The same would apply for a declaration by a file controller to a supervisory authority: a hyperlink would be installed between any site processing personal data and that of the relevant supervisory authority. Finally, consideration might be given to the automatic signalling of any site located in a country offering inadequate protection.

In the future, data subjects must be able to exercise their right of access using an electronic signature. It would be obligatory to structure files so that the right of access was easy to exercise. Additional information, such as the origin of documents and a list of third parties to whom certain data had been supplied, should be systematically available. As noted earlier, increasingly, the personal data accumulated by the vast public and private networks are no longer collected for one or more clearly defined purposes but are stored in the network for future uses that only emerge as new processing opportunities or previously unidentified needs arise. In such circumstances, data subjects must have access to documentation describing the data flows within the network, the data concerned and the various users – a sort of data registry.[66]

It should be possible to exercise online the rights of rectification and/or challenge to an authority with a clearly defined status responsible for considering or maintaining a list of complaints. And the right of appeal

[66] This idea is the subject of two Belgian laws that require the establishment of sectoral committees for networks linked to the National Register (Act of 8 August 1983 establishing a national register of persons, as amended by the Act of 25 March 2003, MB. 28 March 2003, Art.12§1) and to the commercial registration authority (Banque Carrefour des entreprises) (Act of 16 January 2003 establishing the authority, MB. 5 February. 2003, Article 19§4).

should also benefit from the possibility of online referral, exchange of parties' submissions and other documentation, decisions and mediation proposals.

Finally, when individuals concerned wish to challenge decisions taken automatically or notified via a network (such as a refusal to grant a building permit following a so-called e-government procedure), they should be entitled to information, via the same channel, on the logic underlying the decision. For example, in the public sector citizens should have the right to test anonymously any decision-making packages or expert systems that might be used.[67] This might apply to software for the automatic calculation of taxes or of entitlement to grants for the rehabilitation of dwellings.

The principle of encouraging technological approaches compatible with or improving the situation of data subjects

Recommendation 1/99 of the EU Data Protection Working Party – the so-called Article 29 Working Party or Article 29 Working Group – is concerned with the threat to privacy posed by internet communications software and hardware.[68] It establishes the principle that software and hardware industry products should provide the necessary tools to comply with European data protection rules. In accordance with this third principle, regulators should be granted various powers.

For example, they should be able to intervene in response to technological developments presenting major risks. The so-called precautionary principle, which is well-established in environmental law, could also apply to data protection. The precautionary principle may require telecommunications terminal equipment (including software) to adopt the most protective parameters as the default option to ensure that those concerned are not exposed to various risks of which they are unaware and which they cannot assess. Similarly, in accordance with the principle of reciprocal benefits, it is appropriate and not unreasonable to equip telecommunications terminal equipment with log-in and log-out

[67] The same principle applies to private decision makers, subject to the legitimate interests of the file controller (particular relating to business confidentiality, which could limit the duty to clarify the underlying logic of the systems).

[68] Article 29 Working Party, *Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*, DG MARKT 5093/98, WP 17, 23 February 1999.

data bases, as is the case with server-type software used by online businesses and government departments. This would enable users to monitor persons who have accessed their equipment and, where appropriate, identify the main characteristics of the information transferred.

This can be illustrated by one of the provisions of the 2002 Directive on privacy and electronic communications. Article 14 states that where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary, way of protecting personal data from the risks of unlawful processing – risks that have been created by all these new technological options. Going further, it is necessary to prohibit so-called privacy killing strategies,[69] in accordance with the security principle enshrined in Article 7 of Council of Europe Convention 108.[70] The obligation to introduce appropriate technical and organisational measures to counter threats to data privacy will require site managers: to make sure that messages exchanged remain confidential; to indicate clearly what data is being transmitted, whether automatically or by hyperlink, as is the case with cybermarketing companies; and to make it easy to block such transmission.

This security obligation will also require those who process personal data to opt for the most appropriate technology for minimising or reducing the threat to privacy. This requirement clearly has an influence on the design of smart cards, particularly multifunctional cards, such as identity cards.[71] Another example of the application of this principle concerns the structuring of medical files at various levels, as recommended by the Council of Europe.

It might be possible to go further by recommending the development of privacy enhancing technologies, that is tools or systems that take more account of data subjects' rights. Clearly, the development of these technologies will depend on the free play of the market but the state must play an active part in encouraging privacy compliant and privacy enhancing products by subsidising their research and development, establishing equivalent voluntary certification and accreditation

[69] The expression is used by Dinant, 'Law and Technology Convergence', above n. 18.

[70] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, opened for signature 28 January 1981.

[71] On the privacy compliant design of multi-application cards, see Ewout Keuleers and J. Marc Dinant, 'Data Protection: Multi-Application Smart Cards: The use of Global Unique Identifiers for Cross-Profiling Purposes – Part II: Towards a Privacy Enhancing Smart Card Engineering' (2004) 20(1) *Computer Law and Security Report* 22–8.

systems and publicising their quality labels, and ensuring that products considered necessary for data protection are available at affordable prices.[72]

Users' right to full control of terminal equipment

The justification for this principle is obvious. Since these terminals can enable others to monitor our actions and behaviour, or simply locate us, they must function transparently and under our control. Article 5.3 of the 2002 Directive, cited above,[73] offers a first illustration of this point. Those concerned must be informed of any remote access to their terminals, via cookies, spyware or whatever, and must be able to take easy and effective countermeasures, free of charge. The 2002 Directive also establishes the rule that users of calling and connected lines can prevent the presentation of the calling line identification.

Going beyond these examples, we would also argue that all terminal equipment should be configured to ensure that owners and users are fully informed of any data flows entering and leaving, so that they can then take any appropriate action. Similarly, as is already the case under some legislation, possession of a smart card should be accompanied by the possibility of read access to the data stored on the card.

User control also means that individuals can decide to deactivate their terminals at any time. This is important as far as RFIDs are concerned. Data subjects must be able to rely on third parties that vouch that such technical means of remote identification have been fully deactivated.[74]

Users may well apply this principle to firms that are not necessarily covered by traditional data protection rules because they are not responsible for data processing. Examples include suppliers of terminal equipment and many forms of browser software that can be incorporated into terminals to facilitate the reception, processing and transmission of electronic communications. The principle also applies to public and private standard setting bodies concerned with the configuration of such material and

[72] On co-regulatory developments, see Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (London: Ashgate, 2003); Yves Poullet, 'Making Data Subjects Aware of Their Rights and Capable of Protecting Themselves', Conference on the Rights and Responsibilities of Data Subjects, Council of Europe, Prague, 14–15 October 2004 (being published).

[73] See above n. 62 and accompanying text.

[74] Clearly this refers to accreditation arrangements such as those already described as joint regulation, above nn. 36–7 and accompanying text, or to approval issued by the authorities to certain undertakings (i.e. public regulation).

equipment. The key point is that the products supplied to users should not be configured in such a way that they can be used, whether by third parties or the producers themselves, for illicit purposes. This can be illustrated by a number of examples.

First, a comparison of browsers available on the market shows that chattering between them goes well beyond what is strictly necessary to establish communication.[75] Secondly, browsers differ greatly in how they receive, eliminate and prevent the sending of cookies, which means that the opportunities for inappropriate processing will also vary from one browser to another. However, blocking pop-up windows or the systematic communication of references to articles read online or of keywords entered in search engines is apparently impossible, at least in a simple way, on the default browsers installed on the majority of the hundreds of millions of personal computers. Finally, attention should also be drawn to the use of unique identifiers and spyware by suppliers of browser tools and communication software.

More generally, terminal equipment should function transparently so that users can have full control of data sent and received. For example, they should be able to establish, without fuss, the precise extent of chattering on their computers, what files have been received, their purpose and who sent or received them. From that standpoint, a data base automatically ensuring the registration of all entering and outgoing flows appears to be an appropriate tool that is relatively easy to introduce.

In addition to users' right to be informed of data flows, there is the question of whether persons are entitled to require third parties to secure authorisation to penetrate their 'virtual home'. Of relevance here is the Council of Europe Convention on Cybercrime,[76] particularly Article 2 concerning illegal access,[77] and Article 3 about illegal

[75] See J. Marc Dinant, 'Le visiteur visité – Quand les éditeurs de logiciel internet passent subrepticement à travers les mailles du filet juridique' (Winter 2001) 6:2 *Lex Electronica*, available from http://www.lex-electronica.org.

[76] Council of Europe, Convention on Cybercrime, CETS No. 185, opened for signature 23 November 2001.

[77] Article 2 – Illegal access:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

interception.[78] In this case, the identification or identifiability of persons taking part in telecommunications is not a precondition for the Convention's application. Similarly, unauthorised access to a computer system is not confined to hacking into major systems operated by banks or government departments but also concerns non-authorised access to telecommunications terminals, represented in the current state of the art by computers.[79]

In other words, we maintain that placing an identifying number in a telecommunications terminal (or simply accessing this number or some other terminal identifier) generally constitutes unauthorised access. In such a legal context, there can be no question of assessing the proportionality of such actions. Authorisation remains a positive act that is quite distinct from any acceptance that might be inferred from silence or a failure to object. It cannot therefore be assumed – as DoubleClick did[80] – that simply by failing to activate a cookie suppressor users have authorised all and sundry to install this type of information on their terminals.

Privacy, the internet and consumer rights

The routine use of information and communication technologies, formerly confined to major undertakings, and the rapid development of electronic commerce that has multiplied the number of online services have led to a more consumerist approach to privacy. Web surfers increasingly view infringements of their privacy – spamming, profiling,

[78] Article 3 – Illegal interception:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

[79] See, in this context, the excellent article by Léonard, 'E-commerce et protection', above n. 35.

[80] Following a class action brought against it some years ago in the US, DoubleClick's practice is now to send all non-identified terminals an initial non-residual and non-identifying cookie named 'accept cookies'. If the cookie is returned, DoubleClick assumes that the terminal accepts cookies and sends an identifying cookie that remains in place for about ten years (previously thirty). If the cookie is not returned, DoubleClick will indefinitely send the cookie requesting authorisation. An opt-out is available that enables informed users to store a cookie that signifies that they do not accept them.

differential charging policies, refusal of access to certain services and so on – from the standpoint of consumers of these new services.

Thus, in the United States the first hesitant steps towards legislation on data protection in the private sector focused on online consumer protection. We should bear in mind the 2000 report of the Federal Trade Commission,[81] which emphasised the need for privacy legislation to protect online consumers. In Europe, as in America, measures to combat spamming are concerned with both consumers' economic interests and data subjects' privacy.

This convergence between consumers' economic interests and citizens' freedoms opens up interesting prospects. It suggests that the right to resort to certain forms of collective action, which is already recognised in the consumer protection field, should be extended to privacy matters. Such an entitlement to 'class actions' is particularly relevant in an area where it is often difficult to assess the detriment suffered by data subjects and where the low level of damages awarded is a disincentive to individual actions. In addition, many other aspects of consumer law could usefully be applied to data protection. Examples are: the obligations to provide information and advice, which could be imposed on operators offering services that essentially involve the management or supply of personal data, such as internet access providers and personal database servers (case law databases, search engines and so on); the law governing general contractual conditions; and measures to combat unfair commercial practices and competition.

Providing personal data as a condition of access to a site or an online service could be viewed not merely from the standpoint of data protection legislation – does the user's consent meet the necessary requirements and is it sufficient to legitimise the processing in question? – but also from that of consumer law, if only in terms of unfair practices in obtaining consent or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied. Another avenue to be explored is whether consumer product liability for terminals and software

[81] US, Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on 'Privacy Online: Fair Information Practices in the Electronic Marketplace'* (May 2000), available from http://www.ftc.gov/os/2000/05/index.htm. In the US, the Federal Trade Commission, which is very active in the consumer protection field, has played a key role in protecting citizens' privacy. On that issue, see Jan Dhont and María Verónica Perez-Asinari, 'New Physics and the Law: A Comparative Approach to the EU and US Privacy and Data Protection Requirement – Looking for "Adequate Protection"' in F. van der Mensbrugghe (ed.), *L'utilisation de la méthode comparative en droit européen – Usage of Comparative Methodology in European Law* (Belgium: Presses Universitaires de Namur, 2003).

can be extended beyond any physical and financial harm caused to include infringements of data protection requirements. How far is the supplier of browser software whose use leads to breaches of privacy objectively liable for data infringements by third parties?

Conclusions

The debate about privacy and the internet is crucial because of the new risks created by the wide reach and the very characteristics of the internet itself. To address these risks a re-evaluation of the basic principles of legislation is required and new legislation may even be needed to keep up with development and the convergence of technologies. More importantly, new fields of investigation need to be opened up as it becomes clear that legislation can no longer provide all the answers. On the one hand, self-regulation is certainly a complementary source that allows various professional *milieus* (the world of cyber marketing, of access providers, of research services or network operators) to develop more specific solutions that build upon the more general or vague principles in the legislation. These solutions, whether at a national, regional or international level, should be developed, as much as possible, in concert with the other interested actors: consumer representatives, civil liberties associations, and so forth. On the other hand, when looking towards the future, technical norms may well provide the optimal mechanism for locating solutions that display respect for everyone's freedom of choice and privacy. In this regard, it is the responsibility of the authorities charged with data protection to penetrate the forums where important decisions are being taken about technical network infrastructure, communication protocols and the characteristics of our browsers.[82]

We are entering a new generation of privacy laws which must be characterised by the recognition of the technology itself as a third party between data controllers and data subjects. The use of new technologies multiplies the amount of data and the individuals capable of accessing it, increases the power of those who collect and process it, and bridges frontiers. A further factor to be taken into account is the complexity and opacity of this technology. A third party – be it the terminal or the network – now intervenes between individual and data controller. Informational

[82] More and more the specifications of the networks' and terminal functioning are defined by international private organisations without oversight or control by the governments, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN) or the World Wide Web Consortium (W3Consortium).

self-determination calls for a measure of control over this third party. So we underline the need for the internet users to understand and control their ICT environment and for society to control and anticipate the technological developments.

Ideally, these debates should take place at a global rather than national level. The internet is global and as time passes the futility of purely national legislative action becomes clearer. The search for an international consensus is evident. To achieve this, privacy advocates could benefit from the support of new pressure groups such as rights organisations and, especially, consumer organisations. In sum, the debate about privacy and the internet has only just begun. Its significance equals that of the internet itself: it is both global and essential if our freedoms are to survive in everyday life.

5

APEC's privacy framework sets a new low standard for the Asia-Pacific

GRAHAM GREENLEAF

Introduction

The APEC (Asia-Pacific Economic Cooperation) economies have adopted what is now called the APEC Privacy Framework, the most significant international privacy instrument since the EU Privacy Directive of the mid-1990s.[1] APEC Ministers at their November 2004 meeting in Santiago, Chile, announced their endorsement of the Framework, which had been developed over the last two years by APEC's Electronic Commerce Steering Group (ECSG) Privacy Subgroup.[2]

US Secretary of State Colin Powell praised the Framework, warning APEC ministers that a multiplicity of privacy standards could create confusion in the marketplace and impede information flows that the US considers vital to conducting business globally. Powell endorsed 'region-wide

This chapter draws on a number of my articles published in *Privacy Law & Policy Reporter* in 2003–2005: 'Australia's APEC Privacy Initiative: The Pros and Cons of "OECD Lite"' (2003) 10(1) 1; 'APEC Privacy Principles Version 2 – Not Quite so Lite, and NZ wants OECD Full Strength' (2003) 10(3) 45; 'APEC Privacy Principles: More Lite with Every Version' (2003) 10(6) 105; 'APEC's Privacy Standard Regaining Strength' (2004) 10(8) 158; 'APEC's Privacy Framework: A New Low Standard' (2005) 11(5) 121. The *Privacy Law & Policy Reporter* is available at http://www.austlii.edu.au/au/journals/PLPR.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995, *OJ*, L 281, 23 November 1995.

[2] The ECSG is a 'Special Task Group' of the Senior Officials Meeting (SOM) which comes under the APEC Secretariat; see 'APEC Structure – Detailed' available at http://www.apec.org/apec/about_apec/structure.html. The ECSG home page is at http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html. The Privacy Subgroup does not have a home page. There is an old website but its 'data privacy' page, http://www.export.gov/apececommerce/privacy.html, is out of date and does not mention the Framework.

privacy policy compatibility' based on the APEC Framework.[3] The United States' endorsement is a clear signal that APEC must have come up with something rather different from the European Union's Privacy Directive, which has led to tensions between the USA and Europe,[4] and between Europe and Australia.[5]

The significance of the twenty-one APEC economies adopting common information privacy standards cannot be doubted. The APEC economies are located on four continents, account for more than a third of the world's population, half its GDP, and almost half of world trade.

The APEC Privacy Framework[6] consists of a set of nine 'APEC Privacy Principles' in Part III, plus a preamble and scope note in Parts I and II. As a set of information privacy principles the APEC Framework is complete, and we can make an assessment of it. However, Part IV 'Implementation' is unfinished, as it only includes Section A 'Guidance for Domestic Implementation' but does not yet include Section B on the 'cross-border elements', which it states 'will be addressed in the Future Work of the Privacy Subgroup'. As a result of this omission, the full significance of the APEC Framework cannot yet be assessed because we do not know whether or how Section B will affect personal data exports within the Asia-Pacific.

I will explain the APEC Framework and analyse it by comparison with other international privacy standards and privacy laws in the Asia-Pacific. First is a discussion of how the Framework was developed. Second, I examine the APEC privacy principles and definitions supporting them

[3] See Asia-Pacific Economic Cooperation, *APEC Ministers Endorse the APEC Privacy Framework*, Media Release, Santiago, Chile, 20 November 2004, available from http://www.apec.org/apec/news___media/2004_media_releases.html.

[4] For the official EU documents on Safe Harbour, see http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/ index_en.htm; for a jaundiced view see Graham Greenleaf, 'Safe Harbor's Low Benchmark for "Adequacy": EU Sells Out Privacy for US$' (2000) 7 *Privacy Law & Policy Reporter* 45.

[5] Graham Greenleaf, 'Private Sector Bill Amendments Ignore EU Problems' (2000) 7 *Privacy Law & Policy Reporter* 41; Aneurin Hughes, 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)' (2001) 24 *University of New South Wales Law Journal* 270, available at http://www.austlii.edu.au/au/journals/UNSWLJ/2001/5.html; Article 29 Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN, WP 40, 26 January 2001; Peter Ford, 'Implementing the Data Protection Directive – An Outside Perspective' (2003) 9 *Privacy Law & Policy Reporter* 141.

[6] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, November 2004; available from http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html (PDF) (follow link); or in HTML from http://www.bakercyberlawcentre.org/appcc/ which contains the final Framework and some of the previous drafts from 2003 and 2004.

to demonstrate the extent to which they embody a low standard of privacy protection compared with other laws and international agreements. Third, I describe how APEC's implementation proposals are so non-prescriptive that they amount to no standards at all, with the caveat that we do not know what is in the missing 'cross-border elements'. Finally, I ask whether it matters that APEC is proposing a low standard, and conclude with some comments on the likely regional and international significance of the Framework.

Making the Framework – APEC's opaque process

APEC has been moving slowly toward privacy standards since 1995.[7] The first APEC document to consider privacy issues as a matter of regional significance was the *Seoul Declaration for the APII (Asia-Pacific Information Infrastructure)* made at the Senior Officials Meeting on Telecommunications and Information Industry, held in 1995 in Seoul, which included privacy in its 'ten core principles' but otherwise said little. The 3rd APEC Ministerial Meeting on the Telecommunications and Information Industry in 1998 made a *Singapore Declaration* stressing the importance of electronic commerce to APEC, and included privacy as an issue to be considered in relation to consumer confidence in e-commerce. However, there was no specialist APEC group to deal with privacy issues until the 1999 establishment of the APEC ECSG by the APEC Senior Officials meeting in Wellington, New Zealand. The Privacy Subgroup was then established and held a 'mapping exercise' of regional privacy laws in 2002. APEC then moved to develop a regional privacy instrument.

There have been occasional calls since the mid-90s for an Asia-Pacific privacy standard to be developed from APEC structures,[8] and from the distinctive regional form that privacy laws have taken in the Asia-Pacific, described by Waters as 'a third way in data protection'.[9] Europe has successfully developed binding regional instruments in the field of data

[7] Graham Greenleaf, 'Global Protection of Privacy in Cyberspace – Implications for the Asia-Pacific', paper at 'Towards an Asia-Pacific Information Privacy Convention?', 1998 Internet Law Symposium, Science & Technology Law Center, Taipei, Taiwan, 23–24 June 1998 (particularly Part 6), available at http://austlii.edu.au/itlaw/articles/TaiwanSTLC.html; Greenleaf, 'Private Sector Bill Amendments', above n. 5.

[8] Graham Greenleaf, 'Towards an Asia-Pacific Information Privacy Convention' (1995) 2 *Privacy Law & Policy Reporter* 127; Greenleaf, 'Global Protection of Privacy', above n. 7.

[9] Nigel Waters, 'Rethinking Information Privacy – A Third Way in Data Protection?' (2000) 6 *Privacy Law & Policy Reporter* 121.

protection with both the Council of Europe Convention of 1981[10] and the Directive of 1995.[11] It would be a logical and valuable development for the Asia-Pacific, the second region in the world to develop a concentration of privacy laws,[12] to also develop a distinctive regional Convention on data protection.

The privacy principles initiative

It was not until late 2002 that a number of APEC economies started to move APEC processes in the direction of a regional privacy agreement. At a meeting of the APEC ECSG in Thailand in February 2003, Australia put forward a proposal for the development of APEC privacy principles using the OECD privacy principles as a starting point,[13] plus implementation mechanisms which address the issue of inter-country personal data transfers ('transborder data flows' in OECD terminology).[14] A Data Privacy Subgroup was set up comprising Australia (the then chair), Canada, Chile, China, Chinese Taipei (Taiwan), Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States. The United States and Canada have subsequently chaired the subgroup.

The Australian proposal which was used as the starting point for the initiative was based on two documents drafted by Peter Ford, the head of the Information and Security Law Division of the Australian Attorney-General's Department: *APEC Privacy Principles (Version 1)* and *Privacy Implementation Mechanisms (Version 1)*.[15] These proposals reflected views common within the Australian government, and most clearly stated in Ford's own previous writings that 'there is no credible international standard other than the OECD Principles',[16] a sentiment repeated in the only footnote to the APEC Framework's Preamble:

[10] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, opened for signature 28 January 1981.

[11] Directive 95/46/EC of 24 October 1995, above n. 1.

[12] Australian (federal and some states), Canada (federal and some provinces), United States (federal), Hong Kong, South Korea, New Zealand, Taiwan and Japan all now have information privacy legislation, and some countries have sectoral laws as well. They are discussed below.

[13] Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, (1981) 20 ILM 422, adopted 23 September 1980.

[14] These documents can be obtained at http://www.apecsec.org.sg/ in the directory Publications / Publications and Library / E-Commerce.

[15] See above n. 6.

[16] Ford, 'Implementing the Data Protection Directive', above n. 5.

> The 1980 OECD Guidelines were drafted at a high level that makes them still relevant today. In many ways, the OECD Guidelines represent the international consensus on what constitutes honest and trustworthy treatment of personal information.

The Version 1 draft also reflected the Australian government's dissatisfaction with the personal data export limitation approach of the EU's Privacy Directive, and its requirements for external assessments of 'adequacy' of a country's privacy laws, particularly as they have been applied by European institutions to the private sector amendments to Australia's Privacy Act 1988.[17]

The proposals went through nine draft versions. After the first three versions were published on the internet,[18] the chair declared that subsequent versions would not be available outside the subgroup and those with whom it consulted, until a 'consultation draft' was released. The early drafts had attracted some public criticisms.[19] The subsequent drafts did become more widely distributed than the chair intended, but critiques external to the process were and remain very few in number.[20]

The extent of consultation by APEC delegates in their home countries varied widely. For example, in the United States there seems to have been continuing consultation with a range of representative bodies, including privacy advocacy groups. New Zealand included academic experts in one of its delegations to a subgroup meeting. In contrast, Australian consultation was a farce, limited to an hour or so at the start of the process. Australia's Federal Privacy Commissioner was consulted, and there may have been private consultations with business groups, but privacy advocacy organisations were not consulted. A forum during the international Privacy Commissioner's conference in Sydney in September 2003 involved public presentations by proponents of the APEC process, but with no public disclosure of the current draft, so few who attended were meaningfully informed.

[17] Greenleaf, 'Private Sector Bill Amendments', above n. 5; Hughes 'A Question of Adequacy?', above n. 5; Data Protection Working Party, above n. 5; Ford, 'Implementing the Data Protection Directive', above n. 5.

[18] See above n. 6.

[19] Greenleaf, 'Australia's APEC Privacy Initiative'; 'APEC Privacy Principles Version 2', both unnumbered note on p. 91, above.

[20] Other than my own articles cited here, and the submissions of the Asia Pacific Privacy Charter Council and Australian Privacy Foundation (also cited here) based on them, detailed analyses of the APEC proposals (pro or con) have not been published (at the time of writing), insofar as can be determined from searches of Google, Legal Scholarship Network and normal legal bibliographic indices.

To summarise the lengthy drafting history,[21] Version 1 of the APEC Guidelines was already 'OECD Lite'[22] because it did not even include all of the 1980 OECD Privacy Guidelines, and also because those 1980 standards were an inadequate starting point. Version 2 was 'not quite so Lite'[23] including some strengthening of the privacy principles, and moving in the direction of adopting the rest of the OECD guidelines concerning implementation. Versions 3–6 revoked the progress of Version 2, weakening the draft even further than Version 1, a process which appeared (to outsiders) to coincide with serious US participation in the drafting process.[24] Version 8, accompanied by an Explanatory Memorandum, was a considerable improvement, and went some distance toward restoring equivalence with Part II of the OECD Guidelines (OECD's eight privacy principles).[25]

A 'Consultation Draft' (version 9, in effect) was released in April 2004 and submissions requested. Criticisms were made to APEC's ECSG during its consultations by privacy advocates including over twenty recommendations by the Asia-Pacific Privacy Charter Council.[26] According to APEC participants, no other submissions were received, and there is no website providing copies of submissions from which this can be confirmed. The principles in the final Framework are little different from those in the Consultation Draft, so critical submissions had little effect.

The tenth version of the principles, renamed as the APEC Privacy Framework, was then endorsed by APEC Ministers in November 2004 and published, complete except for Part IV (B). The work of the subgroup continues.

APEC is a political grouping which does not have a constitution,[27] and there are no legal requirements for public consultation or transparency.

[21] For details, see Greenleaf, 'Australia's APEC Privacy Initiative'; 'APEC Privacy Principles Version 2'; 'APEC Privacy Principles: More Lite'; 'APEC's Privacy Standard Regaining Strength', all unnumbered note, p. 91, above, based on drafts 1, 2, 6, and 8.

[22] Greenleaf, 'Australia's APEC Privacy Initiative', unnumbered note, p. 91, above.

[23] Greenleaf, 'APEC Privacy Principles Version 2', unnumbered note, p. 91, above.

[24] Greenleaf, 'APEC Privacy Principles: More Lite', unnumbered note, p. 91, above.

[25] Greenleaf, 'APEC's Privacy Standard Regaining Strength', unnumbered note, p. 91, above.

[26] See, e.g., the submission to the ECSG of the Asia-Pacific Privacy Charter Council, *Submission to the APEC Electronic Commerce Steering Group Privacy Sub-Group* (31 May 2004), available at http://www.bakercyberlawcentre.org/appcc/APEC_APPCCsub.htm. The author was the chief drafter of that submission, so the arguments are similar to many made in this chapter. The submission is much the same as that made by the Australian Privacy Foundation (APF) at http://www.privacy.org.au/Papers/APEC0403.rtf.

[27] 'APEC is the only inter-governmental grouping in the world operating on the basis of non-binding commitments, open dialogue and equal respect for the views of all participants. Unlike the WTO or other multilateral trade bodies, APEC has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and

No doubt its processes look more consultative and transparent to governments who are part of the process, but this is essentially an intergovernmental bargaining process where the opportunity for any external input is at the whim of the committee chair or the governments involved in the negotiations.

The membership of national delegations to subgroup meetings changed over time, so the Framework is not the product of an easily identifiable group of people. Some regular members of the subgroup had expertise in privacy issues, including the New Zealand Assistant Privacy Commissioner and the Hong Kong Privacy Commissioner. This process is rather different from the 'expert groups' who were convened to draw up the recommendations for the OECD Guidelines[28] and the Council of Europe Convention.

The nine APEC privacy principles

The nine APEC privacy principles deal with most of the broad topics normally found in international or national sets of privacy principles: collection, quality, security, use, access to, and correction of personal information. The text of the nine APEC privacy principles (I–IX) in Part III (hereafter 'APEC IPPs') and the definitions and exemptions in Part II Scope are included in the Annexure to the chapter. The accompanying 'Commentary' on each, which is sometimes a useful indicator of intended interpretation of ambiguities, should be read.[29] Both are discussed below, with emphasis on where APEC varies from other international standards.

Bases for Criticism

There are five distinct forms of criticism that may be levelled at the APEC IPPs, and I will outline their nature before considering each APEC IPP in light of these criticisms.

(1) *Weaknesses inherent in the OECD principles*: First, the APEC IPPs are based on OECD principles more than twenty years old, and only improve on them in minor respects. The inadequacies of the OECD principles have

commitments are undertaken on a voluntary basis': 'About APEC' from APEC secretariat website at http://www.apecsec.org.sg/apec/about_apec.html.

[28] See, e.g., the description of the OECD process by Justice Michael Kirby (Chair of the Expert Group) in Michael Kirby, 'Privacy Protection, A New Beginning: OECD Principles 20 Years On' (1999) 6 *Privacy Law & Policy Reporter* 25.

[29] APEC, *APEC Privacy Framework*, above n. 6.

been identified by authors over the years.[30] Even the chair of the Expert Group that drafted them, Justice Michael Kirby, has stressed the need for their revision before they are suitable for the twenty-first century.[31]

(2) *Further weakening of the OECD principles*: The Framework is in fact weaker in significant respects than the OECD Guidelines, to some extent in its principles but particularly in its implementation requirements. APEC states that the OECD Privacy Guidelines 'represent the international consensus', but only claims that its Framework is 'consistent with the core values' of the Guidelines,[32] not that they reflect them on all points.

(3) *Potentially retrograde new principles*: The only new principles, 'Preventing harm' and 'Choice', while capable of benign interpretations, carry inherent dangers and have little to recommend them.

(4) *Regional experience ignored*: In discussing the APEC process, then Hong Kong Privacy Commissioner Raymond Tang commented that:

> While the OECD Guidelines and European Union Directives offered a starting point for discussions my inclination is that a more regiocentric set of guidelines will ultimately emerge in the final drafting.[33]

The most obvious source for such development is the actual standards already implemented in regional privacy laws such as the laws of Korea, Canada, Hong Kong, New Zealand, Taiwan, Australia, and Japan over twenty-five years. Principles stronger than those found in the OECD Guidelines are common in legislation in the region, and many occur in more than one jurisdiction's laws. However, APEC has as yet not adopted any of these 'regional' improvements.

(5) *EU compatibility ignored*: Given the difficulties that Australia and the US have in accepting that the EU should judge the 'adequacy' of their privacy laws, it is perhaps understandable that they would not be interested in aiming for an Asia-Pacific standard which is compatible with European requirements. They might also consider that an Asia-Pacific bloc with consistently weaker privacy laws than the EU prefers might make it difficult for the EU to stick to its adequacy requirements. 'Thumbing

[30] E.g. Roger Clarke, 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000), available at http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html; Graham Greenleaf, 'Stopping Surveillance: Beyond "Efficiency" and the OECD' (1996) 3 *Privacy Law & Policy Reporter* 148.

[31] Kirby, 'Privacy Protection', above n. 28.

[32] APEC, *APEC Privacy Framework*, above n. 6, Preamble at [5].

[33] Raymond Tang, 'Personal Data Privacy: The Asian Agenda', paper at 25th International Conference of Data Protection and Privacy Commissioners, Sydney, 10–12 September 2003, available from http://www.pco.org.hk.

one's nose' at the EU is not necessarily an approach that other APEC countries would prefer, so it is worth considering the APEC principles from the perspective of consistency with EU principles (not the same question as 'adequacy' of course). The principles in the EU Directive are also the most widely implemented privacy principles, and for that reason deserve comparison as a standard.

Scope of the principles (Part II)

The Part II definitions are largely uncontentious, if unadventurous.

'Personal information' is defined as 'any information about an identified or identifiable individual'. The commentary clarifies only that the information may be 'put together with other information' to identify an individual and that legal persons are not included. The definition does not cover information which may be used to make contact with a person at an individual level, possibly on the basis of knowledge of their characteristics, even though their identity may not be known (e.g. phone numbers, email addresses and IP addresses). Nor do definitions in other laws and agreements cover this aspect. However, this is an illustration of where APEC's principles look to the past and do not deal with problems of the present and future, so they will probably require revision in the medium term.

'Personal information controller' is defined as meaning 'a person or organization who controls the collection, holding, processing or use of personal information', so there can be multiple controllers. However, organisations acting as agents for another are not to be regarded as responsible for 'ensuring compliance', but their principals are. Agents appear to be exempt from any direct responsibility to the data subject for breaches of the principles (a) by actions contrary to their principal's instructions; and (b) even if they are aware they are in breach.

'Publicly available information' is given a broad definition, including the flexible category of information 'that the individual knowingly makes or permits to be made available to the public'. However, the consequences of the definition are not a total exemption: such information is only excluded from the requirement that individuals be given notice of its collection by third parties collecting it. The APEC principles do not give the collector of publicly available information any right, per se, to disclose the information to others. They can, however, use it for the purpose for which they collect it. They must also take reasonable steps to keep it secure, as it is still personal information.

Personal, family and household affairs are excluded, strangely, from the definition of a 'personal information controller', but there is no further list of exemptions for the press, national security, emergencies etc. The wide differences between APEC economies are used to justify countries ('Member Economies' in APEC-speak) creating local exceptions to the principles unconstrained by any APEC list of categories of allowable exceptions.

Instead, the only limits on allowed exceptions are that they should be (a) proportional to their objectives, and '(b)(i) made known to the public; *or*, (b)(ii) in accordance with law' (emphasis added). This last use of 'or' (rather than 'and') appears extraordinarily broad: it allows laws authorising secret *classes* of exceptions (not just secrecy in implementation, as in some forms of surveillance); and it allows exceptions to be created by a business merely by public notice. In both cases the only check on these exceptions is that proportionality is observed. This appears to be a drafting error, which was pointed out to APEC during its consultations but not changed.[34] For comparison, OECD principle 4 states that exceptions should be as few as possible, and made public.

It is not clear whether these limits on exceptions (weak though they are) also apply to those exceptions already included in the principles (for example, to principle VIII access and correction). They should apply, and it is a weakness that this is not clear.

Each APEC principle 1–IX is now examined in turn.

Principle I Preventing harm

The sentiment that privacy remedies should concentrate on preventing harm ('should be designed to prevent the misuse of such information' and be 'proportionate to the likelihood and severity of the harm threatened') is unexceptional but it is bizarre to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other principles makes it easier to justify exempting whole sectors (for example, small business in Australia's law) as not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the United States).

Limitation to prevention of harm is also dangerous if 'harm' means only loss or damage, as it should also cover distress, humiliation etc. This is not clear from APEC's principles. It is also arguable that there should be a

[34] See Asia-Pacific Privacy Charter Council, *Submission*, above n. 26.

right to privacy in some situations independent of any proven harm, such as where there is the intentional large-scale public disclosure of private facts.

This 'principle' would make better sense in Part IV on implementation, as a means of rationing remedies, or lowering compliance burdens. There is no equivalent to this principle in other international privacy standards, and it is an innovation that should be rejected.

Principle II Notice

APEC says clear 'statements' should be accessible to individuals, disclosing the purposes of collection, possible types of disclosures, controller details, and means by which an individual may limit uses, and access and correct their information. Reasonable steps should be taken to provide notice before or at the time of collection. APEC does not, however, require that 'notice' should be by some explicit form of notice (electronic or paper) given to individuals (and nor do most existing regional laws). It can be argued that in many cases this will be the only form that reasonable steps can take.

APEC is not explicit that notice of collection must be given to a data subject where their personal information is collected by a third party. However, both the specific exemption for publicly available information and the Commentary clearly imply that notice should be given in such circumstances. In this respect APEC's principles are stronger than OECD, which does not have any explicit notice requirement, whether collection is from the data subject or third parties.

The OECD purpose specification principle that 'purposes for which personal data are collected should be specified not later than at the time of collection' is only partly implied by APEC's notice principle. For example, it will not apply where publicly available information is collected.

Principle III Collection limitation

APEC requires only that information collected should be limited to what is 'relevant' to the purpose of collection, but not that only the minimum information should be collected. It shares the weaknesses of the OECD's collection principle which only says 'there should be limits on the collection of personal information'. Existing regional laws are usually more strict, with collection objectively limited to where necessary for the functions or activities of organisations (for example, Hong Kong,

Australian Federal law, New Zealand; the Canadian Federal law is even stricter).

While APEC requires that information be collected by 'lawful and fair means', it does not limit collection to lawful purposes, in contrast with existing regional laws (for example, Australian Federal IPPs, NSW, Hong Kong).

Principle IV Uses of personal information

APEC has adopted the weakest possible test of allowable secondary uses: that they only need be for 'compatible or related purposes'. This is a version of the OECD test of 'not incompatible' purposes. Most existing regional laws are stricter than this, requiring that secondary uses be 'directly related' (Australian Federal and NSW public sectors; New Zealand) or within the 'reasonable expectations' of the data subject (Australian private sector National Privacy Principles (NPPs), Victoria, Northern Territory).

In addition to the usual further exceptions of individual consent and 'where authorized by law', APEC adds 'when necessary to provide a service or product requested by the individual'. This could easily be abused if businesses could have the unrestricted right to determine what information available to them was needed for them to decide whether to enter into a transaction, with no need to notify the individual concerned.

Principle V Choice

APEC requires that, where appropriate, individuals should be offered prominent, effective and affordable mechanisms to exercise choice in relation to collection, use and disclosure of their personal information. 'Choice' has been elevated to a separate principle, an approach not taken elsewhere. Since consent is already an exception to the collection and use and disclosure principles, this choice principle only adds an emphasis on the mechanisms of choice, and could be seen as redundant.

By the caveat 'where appropriate' APEC avoids addressing one of the most difficult issues concerning consent: should users be asked to agree to 'bundled consent' to multiple uses of their personal data in order to obtain goods or services? The elevation of choice to a separate principle does, however, risk interpretations that would allow bundled consent.

The wording of the choice principle does not (and should not) imply that consent can override other principles, so it is not implied that individuals should be able to 'contract out' of the security, integrity, access or

correction principles. It also reiterates that APEC does not require choice in relation to publicly available information, and other exceptions 'where appropriate'.

Principle VI Integrity of personal information

APEC requires that personal information should be accurate, complete and kept up-to-date to the extent necessary for its purposes of use. This is uncontentious, except that (like the OECD), it does not include any deletion requirement.

Principle VII Security safeguards

APEC requires information controllers (not their agents) to take appropriate safeguards against risks to personal data, proportional to the likelihood and severity of the risk and the sensitivity of the information. This is uncontentious, except it is hard to see why agents should not also be liable.

Principle VIII Access and correction

APEC's access and correction rights are made more explicit than the OECD's, but are also subject to explicit exceptions where (i) the burden or expense would be disproportionate to the risks to privacy; or (ii) for legal, security, or confidential commercial reasons; or (iii) the privacy of other persons 'would be violated'. These exceptions are very broad and it does not seem that APEC's requirement of proportionality for exemptions applies to them. However, APEC says individuals should have the right to challenge refusals of access.

The dangers of incorrect information are greater where access is prevented by an exception, but APEC has not addressed the question of whether the right of correction depends on there being a right of access. Nor have most existing laws.

Principle IX (a) Accountability

APEC's requirement that there be an accountable information controller is uncontentious, but is limited by the exclusion of agents from liability (discussed above).

Principle IX (b) Due diligence in transfers

Accountability is coupled in principle IX with a requirement that where information is transferred to a third party (domestically or internationally) this requires either the consent of the data subject (an addition proposed by Japan) or that the discloser exercise due diligence and take reasonable steps to ensure that the recipient protects the information consistently with the APEC principles. This sub-principle was proposed by the United States.

This is a soft substitute for a data export limitation principle, and may leave the data subject without a remedy against any party where the exporter has exercised due diligence but the importer has nevertheless breached an IPP. There is no remedy against the exporter, and none against the importer if it is in a jurisdiction without applicable privacy laws.

What principles are missing? (X and beyond)

To demonstrate the essentially timid and backward-looking nature of the APEC principles, it is useful to consider what is missing. The following list gives some examples of distinct additional principles that have developed in the twenty years since the OECD Guidelines, and are found in more than one of the existing regional privacy laws, and can therefore be said to have become (at least to some extent) a 'standard' that APEC has ignored. Also considered are principles contained in the OECD Guidelines themselves, or in the EU Privacy Directive (and therefore all EU laws), or in the Asia-Pacific Telecommunity's Privacy Guidelines.[35]

Openness

The OECD openness principle requires a 'general policy of openness about developments, practices and policies with respect to personal data' and that 'means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use'. These rights apply to any persons, not only data subjects in relation to their own data, and so are rights which are not covered by APEC's notice principle or its right of access. They are important rights to ensure openness of

[35] The Asia-Pacific Telecommunity's website is http://www.aptsec.org/index.html, but the Guidelines do not seem to have been made public. A copy is on file with the author.

surveillance systems to public scrutiny. Openness principles are found in all Australian jurisdictions, Canada and Hong Kong. APEC has no equivalent.

Collection from the individual

Existing regional Acts require in different ways that collection of personal information should be from the individual concerned, wherever possible (including Canada, Australian private sector, NSW, Victoria, Northern Territory and New Zealand). APEC has no equivalent.

Data retention

A 'limited retention principle', initially supported by New Zealand, Hong Kong, China and Taiwan, was removed by consensus from APEC consideration around draft 8. Some form of such a principle is found in Hong Kong, New Zealand, NSW, and Korea. Why should IPPs allow the unlimited retention of all personal information after it has ceased to have any continuing use to the retaining organisation?

Third party notice of corrections

A right to have recipients of incorrect information informed of corrections is found in the jurisdictions of NSW, New Zealand, Hong Kong and the EU, and the Australian Privacy Commissioner has recommended its inclusion in Australian federal law.[36] APEC has no equivalent.

Data export limitations

Restrictions on personal data exports to places where privacy laws are deficient are already found in the jurisdictions of Québec, Taiwan, Hong Kong (not yet in force), Australia (private sector NPPs), Victoria, Northern Territory, and NSW (not yet in force), as well of course as in the EU. The OECD Guidelines also acknowledged the legitimacy of such restrictions, as discussed below.

[36] Australia, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (March 2005), available at http://www.privacy.gov.au/act/review/index.html.

Anonymity

A right to have transactions remain anonymous where appropriate and practical is already found in the jurisdictions of Australia (private sector NPPs), Victoria, Northern Territory, and NSW (health privacy). The APEC principles, it will be recalled, do not even contain a 'minimum collection' principle, and it would be difficult to argue for anonymity merely from the principle that information collected should be relevant to the transaction.

Identifiers

APEC does not have a principle dealing specifically with limits on the sharing of identifiers. This is found in Australia's private sector NPP 7, Victoria and the Northern Territory and in New Zealand's law.

Automated decisions

The EU Directive provides that an organisation must not make a decision adverse to an individual based on automated processing without a prior review of that decision by a human (Art. 15.1), and the Asia-Pacific Telecommunity has principles to similar effect. No regional laws yet have such a principle although the notice and challenge requirements in the data matching controls in the New Zealand and Australian privacy laws go some way in this direction.

Sensitive information

The OECD Guidelines 'Part One – General' recognise that there may be a need for greater protection of sensitive classes of data (OECD 3(a)). IPPs providing protection for defined classes of 'sensitive' information are found in the privacy laws of Australia's private sector, Victoria, the Northern Territory and the EU.

Public register principles

APEC's definition of 'publicly available information' places no limits on the collection of information from public registers and its subsequent use (but not disclosure). Various regional privacy laws either apply their IPPs to public registers (for example, Hong Kong) or include separate

special 'public register principles' (for example, New Zealand, NSW, Victoria)

This is not an exhaustive survey, only the 'top ten' omissions. I am not arguing that all of these principles should have been included in the APEC Framework, although I think some of them should have been. But it would have at least been reasonable to expect the APEC sub-group to have provided reasons why such well-known IPPs should be excluded from a twenty-first-century privacy standard, rather than ignoring them in their final Framework and its explanatory documents.

Conclusions – a new low standard for IPPs

The principles in APEC's Privacy Framework are at best an approximation of what was regarded as acceptable information privacy principles twenty years ago when the OECD Guidelines were developed. They improve on some OECD IPPs in minor ways, and they are weaker than others in some ways. They do not include the OECD IPPs concerning purpose specification or openness, and are therefore weaker on those counts.

They do not include any principles that were not found in the OECD Guidelines except the 'Preventing harm' and 'Choice' principles, which I have argued above are either unnecessary or counter-productive. Their failure to include any other new principles means, as I argue above, that they ignore the experience of those Asia-Pacific countries that do have privacy laws and have consistently included IPPs which go beyond those of the OECD, and very often share these new IPPs across multiple Asia-Pacific jurisdictions. They therefore do not represent any objective 'consensus' of existing regional privacy laws, unless it is that of the lowest common denominator of every IPP in the region.

They also ignore various IPPs included in the EU Directive and which are therefore standard in European countries. This is not the same question as how many of these IPPs would need to be included in a national law before the EU would be likely to find that law 'adequate' (that is a lower test), but it is indicative of the extent to which the APEC Framework varies from a major source of international norms of privacy protection.

My initial reaction to the first draft of the APEC proposal was that it was 'OECD Lite'.[37] There is nothing in the final Framework to change that assessment.

[37] Greenleaf, 'Australia's APEC Privacy Initiative', unnumbered note, p. 91, above.

What use is 'OECD Lite'?

In the rest of this chapter we will turn to the question of 'does it matter that APEC is proposing a low standard of privacy protection?' Is it valuable or harmful that APEC is advocating a very modest benchmark of privacy protection?

Before doing so, it is worth noting that even if we do conclude that the principles in the APEC Framework might play some useful role as a 'starter kit' for countries that do not have any comprehensive privacy laws, we should ask whether they will have any long-term value beyond that. Is it likely that international privacy standards in a decade or twenty years time will be able to ignore all of the 'missing principles' enumerated above? At the very least, it would seem likely that the APEC principles will need to be revised and strengthened if they are to be a long-term guide to Asia-Pacific countries.

Implementation aspects of the Framework

The aim of the Framework – a floor not a ceiling?

To understand the APEC Framework it is necessary to look at what it does and does not try to do. The Framework is primarily 'intended to provide clear guidance and direction to businesses', mentioning business needs frequently in its Preamble. Although its application to government is mentioned rarely in the Preamble, the commentary on Part II states clearly that the Framework applies to both the public and private sectors. However, in light of the Preamble, it is hard to take seriously that it is intended to apply to governments.

The Preamble speaks of 'ensuring' free flow of information but only of 'encouraging' privacy protection. The final points in the Preamble refer to free flow of information as 'essential', but do not accord this status to privacy protection. These examples of terminology indicate how the Framework has a bias against privacy protection in favour of free flow of information. As discussed below in relation to data export limitations, the OECD Guidelines were more even-handed.

The OECD Guidelines 'Part One – General' explicitly state that they are only minimum standards for privacy protection that may be supplemented in national laws by other principles (OECD 6). The APEC Framework is silent on this question, except that (as previously discussed) it makes generous provisions for national exceptions that may weaken the APEC IPPs. It does not at any point explicitly state that there may or

may not be national strengthening of the principles. At most, we could say that the references to free flow of information as 'essential' indicate a preference that the APEC IPPs should not be strengthened in any way which would restrict such information flows.

On the other hand, Member Economies are not explicitly prevented from adopting privacy rights stronger than the Framework's principles. It is hard to see how the Framework could attempt to impose such a ceiling, since (as discussed above), almost every privacy law enacted in the region is stronger than the APEC IPPs in various ways.

It seems, therefore, that all we can conclude is that the APEC Framework recommends a minimum desirable standard for privacy protection (with exceptions), but not a maximum standard: a floor but not a ceiling for privacy protection.

APEC Part IV's implementation provisions

The implementation aspects in Part IV Section A ('Guidance for domestic implementation'), provisions I–VI, are non-prescriptive in the extreme. They state that members 'should take all necessary and appropriate steps' to identify and remove or avoid 'unnecessary barriers to information flows' (I). They do not require any particular means of implementation of the privacy protections, stating instead that the means of implementing the Framework may differ between Member Economies, and may be different for different principles, but with an overall goal of compatibility between countries (V).

In (II) it is made clear that anything ranging from complete self-regulation unsupported by legislation, through to legislation-based national privacy agencies is acceptable to APEC:

> There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative, industry self-regulatory or a combination of these methods under which rights can be exercised under the Framework.
>
> In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various methods of implementation, including through central authorities, multi-agency enforcement bodies, a network of designated industry bodies, or a combination of the above, as Member Economies deem appropriate.[38]

[38] APEC, *APEC Privacy Framework*, above n. 6, (II) at [31].

What criteria are to be used to measure whether a chosen implementation measure is sufficient to implement the APEC IPPs? APEC only states that a country's privacy protections 'should include an appropriate array of remedies for privacy protection violations, which could include redress, the ability to stop a violation from continuing, and other remedies', and these should be 'commensurate with the extent of the actual or potential harm'. Legislation is mentioned as one means of providing remedies but is not required or even recommended (V). No external means of assessment are suggested.

In contrast, even the OECD Guidelines 'Part 4 National Implementation' state that 'Member countries should in particular endeavour to (a) adopt appropriate domestic legislation' and a range of other means including 'reasonable means for individuals to exercise their rights', 'adequate sanctions and remedies' (including against data export breaches), and for 'no unfair discrimination'.[39] The OECD support for legislation is tepid, but APEC's is non-existent.

Nor does APEC require that there be any central enforcement body (no matter what enforcement approach is adopted), but merely recommends some central access point(s) for general information (II).

APEC advocates education and publicity to support the Framework (III). It advocates 'ample' private sector (including civil society) input into the development and operation of privacy regimes (IV).

Member Economies are also supposed to provide to APEC periodic updates on their Individual Action Plan (IAP) on Information Privacy (VI). There are no provisions for any third party assessments of these IAPs in terms of their compliance with the Framework, and (as yet) no criteria for development of an IAP.

In essence, Part IV exhorts APEC members to implement the Framework without requiring any particular means of doing so, or any means of assessing whether they have done so. The APEC Framework is therefore considerably weaker than any other international privacy instrument in terms of its implementation requirements.

Data export obligations and limitations – OECD and EU approaches

In the OECD Guidelines 'Part 3 – Basic Principles of International Application', guideline 17 explicitly sets out three situations when data export restrictions are acceptable:

[39] OECD, *Guidelines*, above n. 13, 19 (a), (c), (d) and (e).

- where the importing country does not 'substantially observe' the OECD Guidelines;
- where re-export would circumvent domestic laws (in effect, where the receiving country does not have its own data export prohibitions); and
- to protect sensitive data not similarly protected overseas.

The OECD Guidelines require that member countries do not impede the free flow of personal information to other OECD countries that do 'substantially observe' the Guidelines, but also explicitly allow (but do not require) restrictions on data export to countries which do not 'substantially observe' the Guidelines.

The novel, perhaps revolutionary, development in the EU Directive was, while it required that there be free flow of personal information to other EU countries, it also required the prohibition of personal data exports to non-EU countries unless the standards required by the EU for personal data exports were met. In some cases, where the EU's standards were met by a non-EU country, the EU country concerned was not permitted to forbid the export to the non-EU country (thereby guaranteeing a certain degree of free flow of personal information even outside the EU).

APEC's missing 'cross-border elements'

What approach is APEC going to take to these issues? At this point, only informed speculation is possible until the missing Part IV Section B 'cross-border elements' are completed.

It is possible that Part IV Section B may place limits on the strength of regional privacy laws. At this stage the Framework does not require any APEC member to allow data exports to other APEC members who (in some yet-to-be-specified way) implement the Framework. However, the Framework has frequent references to the 'essential' nature of free flows of personal information.

Guarantees of a free flow of personal information to a country as a 'reward' for its observance of minimum levels of privacy protection are an essential feature of all previous international privacy instruments (as outlined above). So it would not be surprising in principle if the APEC Framework attempted to prevent data export restrictions within APEC provided the Framework's standards were 'met'.

This was suggested in Australia's original Privacy Implementation Mechanisms (Version 1) accompanying version 1 of the APEC

principles,[40] which proposed various types of self-certification mechanism for assessing whether Members Economies had implemented the principles, and that such certification 'would be accepted by other economies as a basis upon which personal information could be transferred across national borders.'[41] New Zealand's Assistant Privacy Commissioner distributed a paper in reply proposing external measures of assessing compliance.[42] There has been no further advance of this discussion in the APEC documentation since then, but it is still possible that the Australian proposals or something similar may be revived in Part IV Section B.

As noted, the Framework has a bias for free flow of information over privacy protection: it refers to 'ensuring' free flow of information which is 'essential', but only refers to 'encouraging' privacy protection; it does not include any 'data export limitation' principle, (except the soft US-proposed 'due diligence' requirement of principle IX); it does not even explicitly recognise that there can be legitimate privacy reasons for restricting data exports (a weakness compared with the OECD Guidelines).

If some form of self-assessment of compliance by an APEC economy with the APEC Framework is included in Part IV Section B, will this mean that a data exporter can rely on that self-assessment to constitute 'due diligence'? That may be convenient for exporters and importers, but dangerous for the individuals concerned.

If free flow of personal information within APEC to Framework-compliant APEC economies (whether judged by self-assessment or otherwise) is 'required' by Part IV Section B, what will this mean for countries such as Australia that have data export provisions based on the importing country's law being 'substantially similar' to Australian law?[43] If weak APEC implementations are not 'substantially similar' as a matter of Australian law, will we be 'required' to change our law? More likely, it would depend on Australia's Federal Government willingly and voluntarily changing our law, given the lack of any enforcement structures within APEC. APEC's history of being based on voluntary agreement between economies, and lack of any treaties at APEC level, mean that any suggestion of the APEC Privacy Framework 'requiring' anything of Member

[40] See above n. 6.

[41] See Greenleaf, 'Australia's APEC Privacy Initiative', unnumbered note, p. 91, above.

[42] Blair Stewart, 'A Suggested Scheme to Certify Substantial Observance of APEC Guidelines on Data Privacy', paper at APEC E-commerce Steering Group meeting, 2003, discussed in Greenleaf, ibid.

[43] Privacy Act 1988 (Cth), NPP 9.

Economies must be read as only involving voluntary compliance. Nevertheless, it is possible for countries to voluntarily bind themselves to standards, as the OECD privacy Guidelines have demonstrated to some extent. Voluntary compliance is nevertheless compliance.

These factors give some reason to be cautious and conclude that we do not know what the Framework means until Part IV Section B is completed. It could still contain 'free flow of information' 'requirements' that have the effect of requiring a weakening of existing and future data export laws in the Asia-Pacific.

However, Section B could also turn out to be as innocuous and non-prescriptive as Section A. The 2005 Work Agenda for the ECSG Privacy Subgroup, and the chair's report on the meeting of the Information Privacy Subgroup's meeting in Seoul in February 2005[44] do not include any discussion of development of any mandatory 'free flow' requirements. One of the three work items is 'Cross-border privacy codes: Member Economies will endeavor to support the development and recognition of organizations' cross-border privacy codes across the APEC region', which sounds more like recognition that different countries might have different rules for restricting personal data exports. (These matters were expected to become more clear after the implementation seminar due to be held in Hong Kong in July 2005.)

Regional and global implications of the Framework

The implications of the APEC Framework need to be considered at three levels: effect on APEC countries with no systematic information privacy laws (mainly developing countries, but also countries such as Singapore and Malaysia); effect on APEC countries with existing systematic information privacy laws; and the global implications, particularly the effect on transfers of personal data between the EU and the Asia-Pacific.

The effect on APEC countries with no information privacy laws

If the APEC Framework encourages some of the many regional countries that do not have any significant privacy laws to adopt laws based on the Framework, and they have some reasonable means of enforcement,

[44] Included in Asia-Pacific Economic Cooperation, *Report of the APEC Electronic Commerce Steering Group 11th Meeting*, 2005/SOM I, 24–25 February 2005 (report to the Senior Officers Meeting).

it could have beneficial effects. Even here, beneficial effects will depend upon the Framework not being presented and accepted as a ceiling on either what is allowable or desirable. Since all Asia-Pacific countries with information privacy laws have stronger laws than the APEC IPPs, and stronger implementation than industry self-regulation, it is at least desirable that new countries enacting privacy laws should consider seriously the stronger IPPs and stronger implementations adopted by other APEC economies.

A lot will depend on how the Framework is explained in (or 'sold to') countries with few privacy laws, given that its terms allow virtually any form of implementation from the strongest to the weakest. The US government has allocated US$100,000 to fund the implementation of the Privacy Framework through Technical Assistance Seminars on Domestic and International Implementation, to be conducted by private consultants. The brief given to the consultant, and the extent of supervision by the US government, will be important determining factors.[45] The consultants who have been engaged to develop and present the seminars are the former subgroup chair, Peter Ford, and the former Australian Privacy Commissioner, Malcolm Crompton. The first seminar was due to be held in Hong Kong in July 2005.

The effect on APEC countries with stronger privacy laws

If the concerns expressed here about the missing Section B prove to be unfounded, and the Framework is not regarded as a ceiling on either what is allowable or desirable, then the APEC Framework will not have any explicitly harmful effects on the domestic laws of countries that already have privacy laws.

However, low implementation of the APEC 'standard' may place the few APEC countries such as Australia that have data export limitations in their own laws in the difficult position that these implementations might not be sufficient to justify exports of personal data from Australia.

The global implications

A more detailed comparison between the APEC principles and the EU's requirements for findings of 'adequacy' is needed beyond the simple

[45] Requests by the author to the US Commerce Department for a copy of the brief have not been answered.

observation that the APEC principles are weaker than those of the EU, but is beyond the scope of this chapter. The non-prescriptive approach to implementation and the wide scope for exemptions means that almost everything will depend on national implementations. The relationship between the Framework and the EU Privacy Directive also cannot be answered until the missing Part B is completed and the interaction between the two sets of 'cross-border elements' is known. It seems unlikely that adherence to the APEC Framework will by itself play a significant role in APEC countries obtaining a finding of 'adequacy' by the EU.

Conclusions – a Janus-faced initiative?

My initial reaction to the APEC privacy initiative was that it was Janus-faced. On the positive side, it presents an opportunity for a systematic attempt, backed by APEC, to encourage regional countries with no privacy laws to develop them. There is also the opportunity to develop some level of consistency, even if it is to a relatively low standard, which (optimistically) might only be interim. If the standard was high enough, at least some laws implementing it might provide a reasonable basis for free flow of personal information within the region.

On the negative side there is a danger that the APEC principles will be advocated and accepted as a ceiling on what is desirable in regional privacy laws, and will result in Asia-Pacific countries developing and retaining a generally low standard of privacy protection compared with Europe. The emptiness of the implementation provisions may result in laws which provide no real remedies for individuals but are proclaimed to 'comply with the APEC Privacy Framework' when demands for stronger remedies are raised. There is still a danger that Part 3 Section B may attempt to require (or even just encourage) personal data exports to countries with very weak implementations of the Framework, in the name of 'free flow of information'.

All of these hopes and all of these dangers are still present in the APEC Privacy Framework. Which ones come to fruition will depend on how the missing parts of the Framework are completed, how the consultants carry out their task of facilitating implementations, and ultimately how each APEC economy puts the Framework into practice.

It is nevertheless disappointing that the opportunity has been squandered to encourage a higher standard of privacy protection in the Asia-Pacific. 'OECD Lite' was the wrong place to start, and is the wrong place to end.

Appendix: Text of APEC's privacy principles

[
This text includes Parts II and III of the *APEC Privacy Framework*, November 2004. It omits Part I, the Preamble.]

Part II. Scope

The purpose of Part II of the APEC Privacy Framework is to make clear the extent of coverage of the Principles.

Definitions

personal information means any information about an identified or identifiable individual

personal information controller means a person or organization who controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs

publicly available information means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from:

(a) government records that are available to the public;
(b) journalistic reports; or
(c) information required by law to be made available to the public.

Application

In view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.

Exceptions to these Principles contained in Part III of this Framework, including those relating to national sovereignty, national security, public safety and public policy should be:

(a) limited and proportional to meeting the objectives to which the exceptions relate; and,
(b) i. made known to the public; or,
ii. in accordance with law.

Part III. APEC Information Privacy Principles

I. Preventing Harm

Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

II. Notice

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:

(a) the fact that personal information is being collected;
(b) the purposes for which personal information is collected;
(c) the types of persons or organizations to whom personal information might be disclosed;
(d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;
(e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.

It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.

III. Collection Limitation

The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

IV. Uses of Personal Information

Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

(a) with the consent of the individual whose personal information is collected;
(b) when necessary to provide a service or product requested by the individual; or,
(c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

V. Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

VI. Integrity of Personal Information

Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

VII. Security Safeguards

Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses.

Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

VIII. Access and Correction

Individuals should be able to:

(a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;
(b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;
  i. within a reasonable time;
  ii. at a charge, if any, that is not excessive;
  iii. in a reasonable manner;
  iv. in a form that is generally understandable; and,
(c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

Such access and opportunity for correction should be provided except where:

i. the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;
ii. the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or
iii. the information privacy of persons other than the individual would be violated.

If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

IX. Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When

personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

6

Copyright, privacy and digital rights management (DRM)

DAVID LINDSAY AND SAM RICKETSON

> The combination of tracking technology and online licensing on the one hand, and extra-copyright limitations based in privacy rights on the other, would in my opinion yield a better copyright regime than many national laws now afford with respect to the problem of private copying.
>
> Jane C. Ginsburg[1]

Introduction

The quotation from Jane Ginsburg provides a useful entry point into the subject of this chapter: the relationship between copyright law, privacy laws and the emerging phenomenon of digital rights management (DRM). There can be little doubt that the production and distribution of copyright-protected material in digital form has created challenges for its owners, in particular new horizons for seemingly endless forms of infringement by users. These challenges have, in turn, spawned DRM systems and technologies that are designed to deter infringement and facilitate management of rights in new and different ways and which may well provide copyright owners with more control over their material and over users than was possible in the non-digital environment. The phenomenon of 'digital lock-up' and the restrictions that this may place upon users of copyright material has already received much attention from policy makers and commentators,[2] but a matter that has received less consideration

This chapter arises from work done pursuant to an Australian Research Council (ARC) grant on online privacy.

[1] 'Copyright or "Infograb": Comment on General Report on Limitations Found Outside Copyright' in Libby Baulch, Michael Green and Mary Wyburn (eds.), *The Boundaries of Copyright, its Proper Limitations and Exceptions* (Sydney: ALAI Study Days, Australian Copyright Council, 1999) p. 57.

[2] For a detailed examination of these issues, see the various national reports and comments in Jane C. Ginsburg and June M. Besek (eds.), *Adjuncts and Alternatives to Copyright*, Proceedings of the ALAI Congress, Columbia University, New York, 13–17 June 2001 (2002).

is the subject of the present chapter: the threat that the development of such systems may pose to the privacy of users.[3]

This chapter begins with a brief overview of what is meant by DRM systems, and then considers the following matters: the relationship between copyright and DRM systems, and the extent to which the latter may promote or hinder accepted objectives of copyright protection; the relationship between DRM systems and the privacy of end users; and the broader relationship between copyright and privacy, with particular focus on how potential tensions between the objectives of copyright protection and the objectives of privacy protection may be resolved.

In the light of this analysis, we then address the question of whether or not there is a need for limitations on DRM systems (legal or otherwise) so as to ensure an appropriate balance between the objectives of copyright protection and the protection of end user privacy. In this regard, we maintain that different conclusions may be drawn, depending upon the perspective from which these questions are approached, namely a common law, utilitarian (or 'interests-based') approach (based on 'marketplace norms') and a civil law, rights-based approach (based on 'personhood norms').[4] On the first approach, authors and end users may be regarded as holding only 'interests', which are subsidiary to the promotion of social (economic) welfare. In contrast, on the second approach, authors and end users may be regarded as having 'rights' derived from the autonomy of persons and respect for human dignity. Although the characterisation of 'rights' and 'interests', and the relationship between the two, is notoriously complex,[5] there is general agreement that a fundamental right, such as a right associated with the autonomous development

[3] For an analysis of the relationship from a Canadian perspective, see Ian R. Kerr, 'If Left to Their Own Devices . . . How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy' in Michael Geist (ed.), *In the Public Interest: The Future of Canadian Copyright Law* (Ottawa: Irwin Law, 2005) pp. 167–210.

[4] This distinction draws on Geller's contrast between 'marketplace norms' and 'authorship norms' in the copyright context: Paul Edward Geller, 'Must Copyright Be For Ever Caught between Marketplace and Authorship Norms?' in Brad Sherman and Alain Strowel, *Of Authors and Origins* (Oxford: Clarendon Press, 1994) pp. 159–201; Paul Edward Geller, 'Toward an Overriding Norm in Copyright: Sign Wealth' (1994) 159 *Revue Internationale du Droit d'Auteur (RIDA)* 3. For other views on the contrast between common law and continental copyright traditions see Alain Strowel, 'Droit d'auteur and Copyright: Between History and Nature' in Sherman and Strowel, *Of Authors and Origins*, pp. 235–53; Kamiel J. Koelman, 'Copyright Law and Economics in the EU Copyright Directive: Is the *Droit d'Auteur* Passé?' (2004) 35(6) *International Review of Intellectual Property and Competition Law* 603.

[5] For an overview, see Frances M. Kamm, 'Rights' in Jules Coleman and Scott Shapiro (eds.), *The Oxford Handbook of Jurisprudence & Philosophy of Law* (Oxford: Oxford University Press, 2002) pp. 476–513.

of a person, will prevail over 'interests', such as interests in economic efficiency. Following from this, we conclude that the appropriate form of legal protection – including the potential application of laws to DRM systems – should depend upon whether authors and/or end users are regarded as having 'interests', which must be balanced with other 'interests', or as having 'rights', which will take precedence over mere 'interests'.

Digital rights management

Digital rights management is an imprecise term that can be defined in different ways. One definition is provided in a guide prepared by the Australian Department of Communications, Information Technology and the Arts, which states:

> DRM is a term used to describe a range of techniques that use information about rights and rightsholders to manage copyright material and the terms and conditions on which it is made available to users.[6]

Insofar as this definition limits the term to techniques for protecting copyright material, it is too restrictive, in that DRM systems may also deal with rights in material that is not protected by copyright, including material which is now in the public domain through the expiry of copyright protection. A more satisfactory definition, proposed by Niels Rump, is that:

> DRM covers the description, identification, trading, protecting, monitoring and tracking of all forms of usages over both tangible and intangible assets.[7]

DRM can therefore be properly understood as a series of functions designed to ensure the security of content in order for it to be capable of being traded. As Rump helpfully explains, DRM consists of two groups

[6] Australia, Department of Communications, Information Technology and the Arts, *A Guide to Digital Rights Management* (Canberra: DCITA, 2002) http:www.dcita.gov.au/drm/.

[7] Niels Rump, 'Digital Rights Management: Technological Aspects – Definition, Aspects, and Overview' in Eberhard Becker, Willms Buhse, Dirk Günnewig and Niels Rump (eds.), *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (Lecture Notes in Computer Science Vol. 2770) (Berlin: Springer, 2003) pp. 3–15 at p. 4. Another useful definition of DRM is 'the chain of hardware and software services and technologies governing the authorised use of digital content and management of any consequences of that use throughout the entire life cycle of the content. DRM is an access and copy control system for digital content, such that the DRM securely conveys and enforces complex usage rights rather than simple low-level access/copy controls . . . DRM technologies include a range of functions to support the management of intellectual property for digital resources, such as expression of rights offers and agreements, description, identification, trading, protection, monitoring and tracking of digital content': see Mariemma I. Yague, IASTED International Conference on Communication, Network, and Information Security (New York, NY, 10–12 December 2003), available from http://www.iasted.com.

of functions: the managing of digital rights (or 'management') and the digital management of rights (or 'enforcement'). The functions relating to the management of digital rights include identifying content, defining rights in relation to that content, and defining rules about the way in which that content may be exploited. The functions involved with digital management of rights are those concerned with enforcing the defined rules, including the tracking of content, restricting access to content, and monitoring or restricting use of content.

Following Rump's classification, the typical components of a DRM system are as follows:[8]

1. *Secure containers* designed to make content inaccessible, mainly by means of encryption;
2. *Rights expressions* used to define those to whom access to the secure containers is permitted;
3. *Content identification and description systems* used to uniquely identify the content and attach metadata to the content;
4. *Identification* of people or organisations that intend to interact with the content, usually by means of unique identifiers, so as to limit access to authorised users;
5. *Authentication* of people or organisations that intend to interact with the content, often by means of public key cryptography;
6. Means of persistently associating identifiers and other information to the content, such as *watermarking*. Watermarking is a form of steganography, namely the art or science of hiding secret information. Inserting encrypted data into a file is a means of identifying that file, which corresponds to the forensic application of watermarks. The non-forensic application of watermarks involves their use in ensuring compliance with defined rules. For example, if consumer equipment does not detect a watermark it may not perform the required functions.
7. A means of *reporting events*, such as payment for content; and
8. *Payment systems*, including credit cards and electronic cash.

It can therefore be seen that DRM systems comprise a set of tools that comprehensively define and manage the relationship between content owners (of which copyright owners are a sub-set) and end users, including mechanisms for defining rights over content and mechanisms for enforcing those rights. It is important to bear in mind that not all DRM systems

[8] This classification of DRM components is a paraphrase of the classification proposed by Niels Rump: see Rump, 'Digital Rights Management', above n. 7, p. 7.

will incorporate all of the above functions or components, and that these may also be combined and ordered in a variety of ways.

Copyright and DRM

Before the emergence of DRM systems, the legal relationship between content owners and users was defined mainly by the substantive norms of copyright law, in combination with contract law. Inevitably, these placed limits on what users could do with content; but this was in a 'hard copy' world, with all the attendant physical limitations on the control of content that this entailed. The advent of digital technologies and networking, however, has given rise to a new policy dilemma: do such systems remain consistent with, and advance, the traditional objectives of copyright protection, or do they now overreach these objectives?

In considering this issue it is helpful to review the purposes of copyright protection, and how these have been seen by different western legal traditions, in particular by common law and civil law systems. While we emphasise the clear differences, it is important to note at the outset that there are also important similarities.

In broad terms, there are two ways in which the objectives of copyright protection have been framed in western legal systems: first, by reference to the notion of authors' rights, and secondly by reference to more instrumentalist or utilitarian concepts that view copyright protection as providing incentives for the production of literary and artistic works. The first of these, which is characteristic of civil law jurisdictions, may loosely be described as a 'rights-based' approach, in that it emphasises the rights of authors in their works. The influence of the philosophers Kant and Hegel has been seminal in this tradition, which received its most systematic formulation in the writings of later German legal scholars, such as Gareis, von Gierke and Kohler.[9] In the civil law tradition, the rights of authors have both an economic and non-economic aspect, the latter being called 'moral rights'.

The 'moral rights' of authors can be seen as part of the wider personality rights attaching to individuals by virtue of their status as persons. Indeed, this conception of authors' rights has led civil law jurisdictions historically to draw sharp boundaries around authors and their creations

[9] See, e.g., Edward J. Damich, 'The Right of Personality: A Common-Law Basis for the Protection of the Moral Rights of Authors' (1988) 23 *Georgia Law Review* 1; Neil Netanel, 'Alienability Restrictions and the Enhancement of Author Autonomy in United States and Continental Copyright Law' (1994) 12 *Cardozo Arts and Entertainment Law Journal* 1.

('works') and rights in relation to lesser forms of production of a more industrial or corporate kind that are described as 'neighbouring rights' (sound recordings, broadcasts, performances, and the like). Such notions of authors' rights are not completely unknown in common law jurisdictions, where the natural rights labour theories of John Locke, although somewhat different to the natural rights tradition in civil law jurisdictions, were clearly influential in such early copyright decisions as *Millar* v. *Taylor*,[10] as well as resonating in the early copyright statutes adopted by the newly independent American colonies in the late eighteenth century. But, as explained below, natural rights theories have been much less important in the common law tradition than in the civil law tradition, where the notion of authors' rights has been pervasive.

Authors' rights theories encounter difficulties when the role of the positive laws embodying them is considered in its wider economic and social context. For example, what limitations, if any, are to be placed on the rights so recognised? How wide should rights extend and for how long? If the right in question is a natural right of property, for instance, why should not it be perpetual and universal? Furthermore, authors' rights theories, by definition, have no part to play when considering the scope and duration of neighbouring rights protection. Pragmatic considerations, even in civil law jurisdictions, have therefore always meant that there have been limitations placed on authors' rights that acknowledge a wider public interest in the dissemination and use of the works that have been created.

In contrast to the 'rights-based' tradition, copyright laws in common law jurisdictions have always had a predominantly utilitarian and instrumentalist character in which the grant of exclusive rights has been seen as an essential incentive for the creation and distribution of useful works, rather than as an acknowledgement by positive law of rights already existing in natural law. This notion was neatly encapsulated in the Preamble to the first English copyright statute, the Act of Anne (1709), namely:

> An Act for the Encouragement of Learning, by vesting the Copies of printed Books in the Authors or Purchasers of such Copies, during the Times therein mentioned.

Under such an approach, the grant of rights was to be calibrated for the wider social purpose, the encouragement of learning, which clearly underlined the conditional and instrumental character of the rights conferred. Such instrumentalist analysis has become far more sophisticated since

[10] (1769) 4 Burr. 2303; 98 ER 201.

1709, becoming increasingly couched in the language of economists. It is now fair to say that the economic understanding of copyright has become the dominant influence on copyright policy-making in common law jurisdictions, as well as becoming increasingly influential in civil law systems. A good example of this approach is a recent paper produced by the United States Congressional Budget Office, which explained the purpose of copyright protection in the following terms:

> An economically efficient outcome in markets for creative works is elusive. Efficiency in markets for goods and services generally requires that the cost of producing the last (or marginal) unit must equal society's valuation of it. However, once a copyright work has been created, relatively few costs are incurred in its reproduction and distribution . . . Offering a creative work at the relatively low marginal cost of reproduction and distribution, therefore, would not generate the returns needed to recoup the overall expense of supplying it. To encourage creative works, copyright law has traditionally allowed for licensing rights that enable pricing above marginal cost, while placing a limit on the scope and duration of copyright protection to ensure that creative works eventually become widely available. Copyright law therefore accepts some *static* inefficiency (copyrighted works are typically not distributed as widely as is economically feasible) in the interests of beneficial *dynamic* effects (getting those works created in the first place).[11]

While economic analysis has been useful in making the costs and benefits of copyright protection more explicit it has not, in practice, proved any more effective than natural rights approaches in establishing clear legal limits for such protection. In part, this is because there remain important areas of uncertainty in the application of economic analysis to copyright law. But, in practice, the inexorable tendency from the start of modern copyright laws has been towards expansion: in the scope of the subject-matter protected, the exclusive rights accorded, and in the length of such protection. The last-mentioned is of particular significance: from a modest initial maximum of 28 years for 'books' in 1709, the prevailing term of protection in the European Union, United States and Australia is now the life of the author plus 70 years, with corresponding extended terms for neighbouring rights.

The stated rationales for the extension of copyright protection have remained a relatively undifferentiated mixture of the two approaches to copyright – the need to protect the 'rights' of authors and the need to provide appropriate incentives for them to undertake their socially beneficial

[11] United States, Congressional Budget Office, *Copyright Issues in Digital Media* (Washington, DC: CBO, August 2004) (emphasis in original).

activities.[12] At the same time, neither of the approaches has ever envisaged that protection should be indefinite or infinitely extensible; it has always been accepted that they are subject to limitations. As Numa Droz, the distinguished Swiss delegate stated at the first of the Berne Convention drafting conferences in 1884, 'limits to absolute protection are rightly set by the public interest'.[13] In other words, regardless of whether a 'rights-based' or 'interests-based' approach is adopted, there is an ultimate need to strike a balance between authors and owners, on the one hand, and users, on the other.

The notion of the copyright balance, however, sits much more readily with the 'hardcopy' or analogue world where the nature of physical copies places 'natural' limits on what both owners and users alike may do. But the balance begins to shift, or even slide, as we enter the digital world, with its potential for perfect and endless reproduction and dissemination of copyright material,[14] and confront what has been called the 'digital dilemma'.[15] At first blush this seems to present a problem, as the uncompensated copying of digital material that is now possible appears likely to undermine the traditional objectives of copyright protection: some intervention, legislative or otherwise, therefore seems to be called for to reassert the original balance.

Nevertheless, with every dark cloud there is a silver lining and, even without legislative correction, digital technologies carry with them the potential for exercising far greater control over the activities of users. In the words of one well-known commentator, Charles Clark, the 'answer to the machine is the machine'.[16] First, the ease with which digital information

[12] In practice, these approaches have tended to reinforce each other.

[13] See *Actes de la Conférence internationale pour la protection des droits d'auteur réunie à Berne du 8 au 19 Septembre 1884*, p. 67 (closing speech to the 1884 Conference). See also Georges Koumantos, 'Le droit d'auteur et la rémuneration équitable' [1983] *GRURInt* 424.

[14] See Nicholas Negroponte, *Being Digital* (New York: Knopf, 1995). Paul Goldstein has identified three similar attributes of material in digital form: fidelity, facility and ubiquity: Paul Goldstein, *Copyright's Highway* (revised edn, Stanford: Stanford University Press, 2003) p. 163.

[15] See, e.g., United States, Committee on Intellectual Property Rights and the Emerging Information Infrastructure, *The Digital Dilemma* (Washington, DC: National Academy Press, 2000).

[16] Charles Clark, 'The Answer to the Machine is the Machine' in Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium* (The Hague: Kluwer Law International, 1996). Goldstein points out that, in 1995, when Clark originally coined this term, he was more concerned with the ability of computers to provide new means for connecting authors to users than with allowing content owners to prevent unauthorised reproduction or distribution: Goldstein, *Copyright's Highway*, above n. 14, p. 184.

can be manipulated, such as by encryption, means that access or use of such material can be restricted to those with the necessary authority, such as a decryption key. Secondly, the attachment of 'meta-information' to digital material, such as identifying information, establishes the potential for access to, and use of, this material to be closely tracked and monitored. These two categories of response form the basis for all potential DRM systems[17] and, as copyright owners have begun to explore these possibilities, copyright laws at the national, regional and international levels have come to their assistance with additional forms of protection.

This development has been relatively rapid, post-dating the adoption of the TRIPS Agreement in 1994. Separate policy processes at the national and regional level began at this time in such places as the United States,[18] Europe,[19] and Australia,[20] and led, within a very short timeframe, to the adoption of the two WIPO 'Internet Treaties'[21] at the Diplomatic Conference held in Geneva in December 1996. Included in these two instruments were two important new provisions that have specific relevance to DRM systems, namely provisions on anti-circumvention measures and rights management information (RMI).

The first of these, contained in Article 11 of the WIPO Copyright Treaty and repeated, with necessary modifications, in Article 18 of the WIPO Performances and Phonograms Treaty, provides:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law.

[17] For a (dated) survey of DRM systems see: European Commission, *Digital Rights: Background, Systems, Assessment*, Commission Staff Working Paper, SEC(2002) 197, 14 February 2002.

[18] US, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights Information Infrastructure Task Force* (Washington, DC: United States Department of Congress, 1995).

[19] European Commission, *Copyright and Related Rights in the Information Society: Green Paper from the European Commission to the European Council*, COM/95/0382 final, 19 July 1995.

[20] Australia, Copyright Convergence Group, *Highways to Change – Copyright in the New Communications Environment* (Canberra: AGPS, 1994)

[21] So called by Ficsor in his treatise: Mihaly Ficsor, *The Law of Copyright and the Internet: The 1996 WIPO Copyright Treaties, their Interpretation and Implementation* (Oxford: Oxford University Press, 2002).

As for RMI, Article 12(1) of the Copyright Treaty provides that:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:
>
> (i) to remove or alter any electronic rights management information without authority;
> (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

It will be seen that both provisions provide for collateral forms of protection for copyright owners that are essentially directed at the new technological environment in which works and subject-matter are exploited. In other words, these two provisions set the international norms for national laws that apply to DRM systems.

As to the first, it will be seen that this is concerned with the actual technological measures that copyright owners may adopt to protect themselves against unauthorised uses and seeks to penalise actions taken by users to circumvent those measures. The international standard to be applied here is somewhat open-ended, leaving considerable flexibility for national implementation. For example, does it cover attempts to circumvent access control devices, bearing in mind that copyright owners' rights do not include a specific right of access in the non-digital environment? Or is it limited to attempts to circumvent measures that limit use, such as copy controls? And can there be exceptions for certain kinds of circumventing activities, at least where these parallel activities would be allowed in the non-digital environment under the relevant copyright exceptions and limitations in national laws?[22]

These are issues that have received differing responses at national and regional levels, and there has been much controversy as to whether such measures are really consistent with the traditional objectives of copyright

[22] The proper scope of exceptions to anti-circumvention provisions is being reviewed in Australia as a result of changes to the anti-circumvention law that are required to be made by the *Australia–U.S. Free Trade Agreement*. The issue has been the subject of a Parliamentary Committee report: House of Representatives Standing Committee on Legal and Constitutional Affairs, *Inquiry into Technological Protection Measures (TPM) Exceptions* (Canberra: House of Representative, 1 March 2006).

protection or whether they have gone too far.[23] Unfortunately, prior to their introduction, anti-circumvention laws were not subject to rigorous analysis from either a 'rights-based' or 'interests-based' perspective. From a 'rights-based' perspective, it might be thought that any efforts to protect authors against widespread uncompensated copying should be supported. This, however, ignores the limitations on protection historically allowed by civil law systems as a practical concession to the public interest in the dissemination and use of copyright material.

While it is difficult to apply a 'rights-based' analysis to anti-circumvention provisions, some attempts have been made to apply an economic analysis to such laws. According to Landes and Posner, for example, an important economic objective of such measures should be seen as reducing socially wasteful expenditure on the technological 'war' between copyright owners and developers of circumvention techniques.[24] In the absence of anti-circumvention provisions, copyright owners would be likely to over-invest in technological forms of protection, and potential copyright infringers would likewise over-invest in circumvention technologies.[25] The need to contain expenditure on this technological 'arms race' therefore establishes a prima facie case for anti-circumvention laws. The same authors, however, go on to caution that unconstrained implementation of technological forms of protection, such as encryption, may result in inefficiencies in the form of rent-seeking behaviour by copyright owners pursuing more returns than are available under copyright law.[26]

[23] This issue, with the associated ambiguous drafting of the current Australian anti-circumvention provision, caused the Australian High Court considerable difficulty in the main Australian anti-circumvention case, *Stevens* v. *Kabushiki Kaisha Sony Computer Entertainment* (2005) 221 ALR 448.

[24] William M. Landes and Richard A. Posner, *The Economic Structure of Intellectual Property Law* (Cambridge, Mass.: Harvard University Press, 2003) pp. 44–5.

[25] The economic rationale for anti-circumvention provisions therefore bears some similarity to the rationale for trade secrets laws, which can be seen as minimising socially wasteful expenditure that would otherwise be incurred in a 'war' between owners attempting to protect secret information and intruders attempting to obtain the information. In fact, as Friedman et al. point out, an optimal trade secrets law must balance the relative social costs of keeping and discovering secrets, on the one hand, and the costs of a legal system for protecting secrets, on the other: David D. Friedman, William M. Landes and Richard A. Posner, 'Some Economics of Trade Secret Law' (1991) 5 *Journal of Economic Perspectives* 61. This suggests that, in assessing anti-circumvention laws, the costs of such laws should also be taken into account.

[26] To an extent, Ginsburg was referring to this problem when she observed that: 'Copyright owners . . . have eyed enhanced prospects for global earnings in an increasingly international copyright market. Accordingly, they have urged and obtained ever more protective legislation, that extends the term of copyright and interferes with the development and

This leads them to the conclusion that, from an economic perspective, the preferred form of anti-circumvention provision would 'punish the use of circumvention technology only when it was used to infringe copyright',[27] and not when the technology is used to restrict otherwise lawful uses. This distinction, while attractive, is something of a counsel of perfection that has proved difficult for national legislators to implement. The analysis of Landes and Posner also reinforces the difficulties involved in developing an adequate policy framework for regulating the use of technological forms of protection.

For the purposes of our present discussion, it suffices to say that the new provisions at international and national level dealing with circumvention measures are directed at protecting the exploitation of copyright material in the digital environment. They are concerned with guarding the gateways and exit points of the material that is the subject of DRM systems. To date, however, neither an approach based on protecting the dignitarian 'rights' of authors, nor an 'interests-based' approach, has proved capable of providing clear practical guidance as to the appropriate limits on laws prohibiting circumvention measures.

The provisions dealing with RMI, on the other hand, have a more obvious application to DRM systems themselves, being concerned with the identifying information that is added by owners and the knowing removal or alteration of that information. This is not directly concerned with users at all, but only with owners and their 'electronic markings'; the requirement of knowledge and the need to link this to an infringing act is a significant limiting factor. Although more detailed than the anti-circumvention provision, implementation at national level does not appear to be particularly onerous.

More generally, it must be said that neither provision, nor their counterparts at national and regional levels, touches upon the potential impact that their application may have upon users of the copyright material that is so protected and marked, in particular with respect to the privacy of these persons. This is hardly surprising, as the provisions appear in treaties and laws concerned with the protection of authors and owners of copyright materials. But the digital environment gives rise to a potential conflict that was not entirely apparent in the hard copy world: the extent to which

dissemination of consumer-friendly copying technologies': Jane C. Ginsburg, 'How Copyright Got a Bad Name for Itself' (2002) 26 *Columbia Journal of Law and the Arts* 61, 61–2. On the economics of rent-seeking behaviour generally see: Gordon Tullock, *The Economics of Special Privilege and Rent Seeking* (Dordrecht: Kluwer, 1989).

[27] Landes and Posner, *The Economic Structure*, above n. 24, p. 45.

the privacy of end users may justify legal limits on copyright owners protecting their material in the digital environment. Before turning to this issue, however, we need to explain the relationship between privacy laws, especially data protection laws, and DRM systems.

Privacy and DRM

Privacy is acknowledged to be a complex concept, aptly described as 'elusive'.[28] While it is almost universally acknowledged that privacy is connected to the protection of human dignity and individual autonomy, there is wide-ranging debate among scholars and practitioners as to how best to define it.[29] As a starting point, however, it should be noted that privacy is protected as a human right in several important international instruments. Thus, Article 17 of the International Covenant on Civil and Political Rights provides:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

And at the regional level, Article 8(1) of the European Convention on Human Rights (ECHR) provides that:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

None of these general statements, however, provides specific guidance as to the content of the concept of 'privacy'. We therefore need to consider how this matter has been treated, in practice, by different legal traditions.

Here, as with copyright laws, it is possible to see two broad approaches: those that conceive privacy as a fundamental human right and those that view it in a more instrumentalist or 'interests-based' fashion. Again, the first of these is to be found more fully expressed in the civil law tradition,

[28] See Australian Law Reform Commission (ALRC), *Privacy*, Report No. 22 (Canberra: AGPS, 1983), vol. 1 at p. 10.

[29] Important collections of philosophical and legal articles dealing with the concept of privacy include: J. Roland Pennock and John W. Chapman (eds.), *Privacy* (series: Nomos XIII; New York: Atherton Press, 1971); John B. Young (ed.), *Privacy* (New York: Wiley, 1978); Ferdinand Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984); Raymond Wacks (ed.), *Privacy: Volume I* (Aldershot: Dartmouth; New York: New York University Press, 1993). See also David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) *Melbourne University Law Review* 179.

while the second is more typical of common law jurisdictions. The two approaches may be considered in turn.

Continental traditions of privacy protection

The protection of privacy in France can be traced to concerns associated with the liberalisation of the press during the French Revolution. These concerns were concisely expressed by the French philosopher, Royer-Collard, in a well-known 1819 speech, in which he coined the phrase 'private life must be walled off'.[30] From the mid nineteenth century, in a series of cases, French courts developed the concept of the 'right to one's image' (*droit à l'image*), which was eventually formulated as a 'sacred and inalienable right over ourselves, and consequently over the reproduction of our image'.[31] From this time on, French courts continued to protect 'private life' against undue publicity, regarding privacy as a personality right.[32] While this was initially protected through the application of general tort principles, in 1970 an express right to privacy was introduced into French law with the adoption of Article 9 of the French Civil Code, which provides that: 'Everyone is entitled to respect of private life'.[33]

One commentator has recently noted that the early French approach to privacy protection developed in response to threats to traditional notions of honour posed by press freedom in the context of increased sexual liberation in mid-nineteenth-century France.[34] According to this view, French privacy law effectively replaced duelling as the means of protecting the honour or dignity of a person whose privacy was invaded. In this sense, the general protection of privacy extended to all members of French society a dignitarian interest that was previously the preserve of the aristocracy.

By contrast, the German approach to privacy drew on a more systematic theoretical analysis that conceived of privacy as part of the complex area of personality law. Late nineteenth-century German personality law was the result of the application of German idealist philosophy,

[30] Cited by James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151 at 1173.

[31] This formulation was adopted in the famous case of *Dumas c. Liebert*, CA Paris, May 25 1867, 13 APIAL 247 (1867), cited in Whitman, 'The Two Western Cultures of Privacy', above n. 27, 1177.

[32] See, e.g., Elisabeth Logeais and Jean-Baptiste Schroeder, 'The French Right of Image: An Ambiguous Concept Protecting the Human Persona' (1998) 18 *Loyola of Los Angeles Entertainment Law Journal* 511.

[33] Code civil [C. civ.], Art. 9 (Fr.).

[34] Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1179–80.

and especially Hegelian philosophy, to the Roman law of insult. On this approach, the law was seen in evolutionary terms as extending protection to intangible, non-economic interests. As Whitman has explained this development:

> The modern world was now producing what Jhering called, in a famous 1885 article, the law of 'insulting tortious injuries'. In particular, modern protections were now evolving beyond protections against immaterial verbal insults, to include the protection of such immaterial goods as one's name and one's photographed image, one's control of one's correspondence, as well as access to modern amenities such as the telegraph and tram.[35]

The German approach to privacy protection can be traced to much the same nineteenth-century jurisprudential tradition as the development of authors' rights. Thus, while privacy was concerned to protect the personality of an individual against insult, authors' rights were designed to protect the personality of the individual *qua* author as embodied in a particular literary or artistic work. Underlying the civil law tradition of both privacy and authors' rights protection therefore, are concerns with the protection of the dignity (or honour), and autonomy, of the human subject.

In Germany, following the Second World War, in the case of privacy, this found expression in Article II of the *Basic Law ('Grundgesetz')*:

> Every person has the right to free development of his personality, insofar as he does not injure the rights of others or offend against the constitutional order or the moral law.[36]

The constitutional protection of personality rights subsequently formed the basis for the development of German data protection law, especially in the decision of the German Constitutional Court in the 1983 *Census* case.[37] That case concerned the German Census Act of 1983, which required the collection of detailed information for social planning purposes. The Constitutional Court held that, in certain respects, the legislation infringed provisions of the German *Basic Law*, namely Article I(1) which establishes the central constitutional value of human dignity, and the protection of personality rights under Article II. In recognition of the need for fundamental constitutional values to adapt to technological

[35] Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1184 citing Rudolph von Jhering, *Rechtsschutz gegen injuriose Rechtsverletzungen* (1886) p. 236.

[36] *Grundgesetz*, Art. II, para. 1 (Ger.).

[37] 65 BVerfGE 1 (1983).

change, the Constitutional Court authoritatively formulated a constitutionally guaranteed 'right to informational self-determination', essentially meaning 'the authority of the individual to decide fundamentally for himself, when and within what limits personal data may be disclosed'.[38] The decision therefore acknowledged that the preservation of human dignity and individual autonomy required a degree of individual control over data processing.[39] In this respect, the court stated that:

> . . . an individual must be protected against unlimited collection, storage, use and transmission of personal data . . . as a consequence of the free development of personality under modern conditions of data processing.[40]

The approach adopted in the *Census* decision is an essential part of the conceptual background to the 1995 European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (the 'Data Protection Directive'),[41] which established new benchmarks for the protection of personal data of European Union citizens. The Data Protection Directive approaches the regulation of data processing from within the European framework of fundamental rights and freedoms, thereby establishing a 'high level' of protection of personal data,[42] treating this as a matter integral to the protection of the fundamental underlying values of human dignity and moral autonomy.

Common law traditions of privacy protection

Common law approaches to privacy protection have been more fragmented and pragmatic than in civil law jurisdictions. Until recently, English-influenced common law systems did not recognise privacy as an independent value deserving of protection in its own right. When faced

[38] 65 BVerfGE 1 at 42 (1983). The 'right to informational self-determination' was prefigured in earlier decisions, including *Microcensus*, 27 BVerfGE 1 (1969) and *Divorce Records*, 27 BVerfGe 344 (1970).

[39] As Eberle explains the decision: 'At the root of the Constitutional Court's decision was the vision that human dignity and autonomy must be preserved against the onslaught of the modern computer age': Edward J. Eberle, 'Human Dignity, Privacy, and Personality in German and American Constitutional Law' [1997] *Utah Law Review* 963 at 1004.

[40] 65 BVerfGE 1 at 43 (1983).

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, *OJ*, L 281, 23 November 1995, 1.

[42] Thus, Recital (10) to the Directive states that: 'Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy . . . whereas for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.'

with facts that raised issues relating to personal privacy, courts in such systems adopted the conventional practice of listing all causes of action that might incidentally protect privacy, then attempting to fit the facts within one or more of the listed actions.[43] In the words of two distinguished comparative lawyers, contrasting the protection traditionally according to privacy under English common law with that under German law:

> English law, on the whole compares unfavourably with German law . . . The harsh condemnation of English law, should be mitigated by the fact that many aspects of the human personality and privacy do receive some or adequate protection through a multitude of existing torts and specific statutes . . . this means fitting the facts of each case in the pigeonhole of an existing tort, the process often involving strained constructions or, even, leaving deserving plaintiffs without a remedy.[44]

Although English law failed historically to recognise an express right to privacy, the equitable action for breach of confidence was sometimes relied upon to restrain the publication of private material. Indeed, in one of the well-known early cases, *Prince Albert* v. *Strange*,[45] Lord Cottenham LC went so far as to observe that 'privacy is the right invaded'.[46] Moreover, following the introduction of the Human Rights Act 1998 (UK), the protection of privacy under English law has been transformed. Thus, in *Campbell* v. *MGN Ltd*,[47] the House of Lords recognised a right to privacy, in the form of protection against the publication of private facts that fell within the expanded parameters of the action for breach of confidence.[48] One way to interpret this development is as a creative, but potentially fraught, fusion of a 'rights-based' conception of privacy, reflecting the influence of the European Convention on Human Rights,[49] with the traditional incremental approach of the English common law.

[43] See, e.g., *Kaye* v. *Robertson* [1991] FSR 62; *ABC* v. *Lenah Game Meats* (2001) 208 CLR 199.

[44] Basil S. Markesinis and Hannes Unberath, *The German Law of Torts: A Comparative Treatise* (4th edn, Oxford: Hart, 2002) p. 478.

[45] (1849) 1 Mac & G 23; 41 ER 1171.

[46] (1849) 1 Mac & G 23 at 47; 41 ER 1171 at 1179. This statement was made in the context of the rejection of a contention that an injunction could not be awarded until the plaintiff had established proof of title to the property, Lord Cottenham LC pointing out that postponing the injunction would deny the plaintiff's right to privacy.

[47] [2004] 2 AC 457.

[48] See David Lindsay, '*Naomi Campbell* in the House of Lords: Implications for Australia' (2004) 11(1) *Privacy Law & Policy Reporter* 4.

[49] Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952). The continental approach to privacy has been influential in decisions of the European Court of Human Rights interpreting Art. 8: see, e.g., *Von Hannover* v. *Germany* (2005) 40 EHRR 1.

The protection of privacy by means of an extended action for breach of confidence under English law may be contrasted with the cautious recognition of a tort of public disclosure of private information under New Zealand law in *Hosking* v. *Runting*.[50] In that case, a majority of the New Zealand Court of Appeal appeared to adopt a 'rights-based' analysis by referring to a 'shift in emphasis' in tort liability from liability for reprehensible conduct to the protection of identified rights.[51] The New Zealand public disclosure tort, in turn, has clear parallels to much earlier developments in the United States, where aspects of 'privacy' have long been protected under the law of torts.

As is well known, the protection of privacy in the United States received its impetus from the seminal article of Samuel D. Warren and Louis D. Brandeis, entitled 'The Right to Privacy', published in the *Harvard Law Review* in 1890.[52] Although the article cited many earlier English precedents, including *Prince Albert* v. *Strange*, it was also clearly influenced by late nineteenth-century German personality law, with the central argument in the article being that the proposed right to privacy and an author's rights over literary or artistic works had common roots in 'the more general right to the immunity of the person, the right to one's personality'.[53] Writing over 70 years after Warren and Brandeis, Prosser was able to categorise four species of privacy-protecting torts that had been developed by US courts in the intervening period: intrusion upon seclusion; misappropriation of name or likeness; public disclosure of private facts; and portrayal of the victim in a false light.[54] Not all of these torts have flowered to full maturity in US law: most significantly, the importance accorded to the First Amendment protection for freedom of expression has rendered the public disclosure and intrusion torts all but illusory.[55] But for our purposes, the influence of the civil law tradition on the initial recognition of privacy as a right under American common law is what is significant.

[50] [2005] 1 NZLR 1.

[51] Ibid. [2] (Gault P and Blanchard J).

[52] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

[53] Warren and Brandeis, 'The Right to Privacy', ibid. 207. Moreover, the article expressly refers to the nineteenth-century German interpretation of the Roman law in Salkowski's text, *Institutes and History of Roman Private Law* (Warren and Brandeis, 'The Right to Privacy', p. 198 n. 1).

[54] William Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

[55] See, e.g., Diane L. Zimmerman, 'Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort' (1983) 68 *Cornell Law Review* 291; Rodney A. Smolla, 'Accounting for the Slow Growth of American Privacy Law' (2002) 27 *Nova Law Review* 289.

As Whitman suggests, 'it is best to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant'.[56] In an interesting modern parallel, we are now seeing a discernible civil law influence on contemporary developments in the English action for breach of confidence. It can therefore be seen that, while common law courts have sometimes loosely referred to a 'right to privacy', the recognition of privacy as a fundamental 'right' in the common law tradition has been partial at best and, where this has occurred, it has been influenced by conceptions of privacy drawn from the civil law tradition.

The differences between the common law and civil law approaches can also be seen in differences in the legislative reaction to the emergence of large-scale computerised databases in the 1960s and 1970s. Practical concerns that different national standards would inhibit the growth of transborder flows of personal data led to the development of data protection laws, marked by the adoption of the 1980 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the 'OECD Guidelines').[57] Since then, however, there has been a significant divergence in approaches to data protection laws, seen most clearly in the difference between the European and American approaches.

With its strong 'rights-based' background, the European Union adopted a 'high level' of protection in the 1995 Data Protection Directive. The United States, by contrast, has refrained from legislating comprehensively with respect to information privacy, instead enacting laws on an ad hoc basis to deal with problems as they have arisen in specific sectors. Data processing is therefore largely left to be regulated by the market or by industry self-regulation. As one commentator has explained, under the US approach:

> Regulation is perceived to intrude on the commitment to freedom from government interference in information flows. As a result, law emphasizes regulation of the market process rather than the substantive contours of information privacy.[58]

In other common law jurisdictions, such as Australia, data protection laws have been based on the standards established by the 1980 OECD

[56] Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1204.

[57] Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1981) 20 ILM 422, adopted 23 September 1980.

[58] Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review* 1315 at 1343.

Guidelines, which were a pragmatic attempt to balance the competing values of information privacy and the free flow of information. This can be seen, for example, in section 29(a) of the Privacy Act 1988 (Cth), which imposes a statutory duty on the federal Privacy Commissioner to 'have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information . . . and the recognition of the right of government and business to achieve their objectives in an efficient way'.

In practice, we see a spectrum of approaches across jurisdictions to data protection, ranging from the strong, 'rights-based' approach embodied in the EC Data Protection Directive, to the US preference for relying on market forces rather than the law to protect personal information. But the main point is that legal systems drawing on the common law tradition, when compared with civil law systems, have tended to privacy more as an 'interest' than as a fundamental right, thereby providing weaker privacy protection.

How, then, do these different legal approaches impact on the use of personal information that may be collected through DRM systems?

Application of the two privacy traditions to DRM

Of the identified functions or components of DRM systems, the following may raise privacy concerns:

1. *Identification* and *authentication* of end users of protected content;
2. The *reporting of events* relating to access to, or use of, protected content; and
3. The *rule sets* as a whole, which define the conditions relating to access to, or use of, protected content.

The three main privacy-related concerns raised by these functions are, respectively:

1. The potential for unconstrained collection and processing of identifying information;
2. The potential for persistent surveillance and monitoring of end users of protected content; and
3. The potential for direct constraints to be imposed on the use of protected content, including restrictions on 'private' uses of content.

Each of these deserves further investigation.

Collection and processing of identifying information

Many DRM systems, like electronic commerce systems more generally, involve the collection and/or processing of information that relates to end users. This information may be collected or processed for purposes such as secure delivery of content, payment mechanisms, customisation or personalisation of content, or user profiling. Potentially identifying information collected by DRM systems takes a variety of forms. It may, for example, consist of credit card information, a digital signature, an email address, an Internet Protocol (IP) number or 'clickstream data'.[59] The identifying information may be collected or processed either with the knowledge of the end user, or without the end user knowing.

As explained above, the revolution in information processing made possible by the computer led to the development of data protection laws in the 1970s. There are two legal issues that arise in the application of data protection laws to information that is collected or processed by DRM systems:

1. The scope of the information regulated by the laws; and
2. If information is regulated by the laws, the nature of the rules, or principles, that apply to the collection and processing of personally identifying information.

The approach taken to these issues can be seen to depend upon whether a 'rights-based' or 'interests-based' approach is taken to the protection of privacy, and is well-illustrated by comparing the 'rights-based' EC Data Protection Directive with the predominantly 'interests-based' approach embodied in the Australian Privacy Act 1988.[60]

[59] 'Clickstream data' may be defined as: 'A virtual trail that a user leaves behind while surfing the Internet. A clickstream is a record of a user's activity on the Internet, including every Web site and every page of every Web site that the user visits, how long the user was on a page or site, in what order the pages were visited, any newsgroups that the user participates in and even the e-mail addresses of mail that the user sends and receives': see http://www.webopedia.com. An indication of the information trail left by internet users may be obtained from the sites: http://privacy.net/analyze/ or http://www.cnil.fr/uk/index.htm.

[60] While the Preamble to the Privacy Act expressly refers to Art. 17 of the ICCPR, the substantive provisions of the Act appear to be based on the view that privacy is an 'interest' to be balanced with other interests. The 'interests-based' approach to data protection is confirmed by the terms of reference for the Privacy Commissioner's 2005 review of the private sector provisions of the Privacy Act, which refer to 'individuals' interests in protecting their privacy' and 'important human rights and social interests that compete with privacy': Australia, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (March 2005), Appendix 1.

First, the scope of data protection laws is set by the definition of 'personal information' (or 'personal data'). Laws that adopt a 'rights-based' approach to data protection appear to have a broader scope than laws with an 'interests-based' perspective. Thus, the term 'personal data' is defined by the Data Protection Directive to mean:

> . . . any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[61]

The Australian Privacy Act, by contrast, defines 'personal information' as:

> . . . information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.[62]

Two potential problems have been identified with the Australian definition: it is not clear whether it applies to video images that are not directly referenced to other information identifying an individual; and it does not seem to apply to online information, such as an email or IP address, that does not identify an individual, but allows an individual to be contacted.[63] The first problem seems to be dealt with by the definition of 'personal data' in the Data Protection Directive, which expressly applies to information that may *indirectly* identify the data subject. The second problem is much more relevant to the potential application of data protection laws to DRM systems, which may well collect information that identifies an address or machine, but not the identity of an individual. In this respect, it can be noted that the European Union, in its 2002 Directive on Privacy and Electronic Communications,[64] introduced a form of prior notice and consent for the processing of online 'tracking' information that do not necessarily identify the data subject. To this effect, Article 5(3) of the Directive provides that:

[61] Data Protection Directive, above n. 41, Art. 2(a). [62] Privacy Act 1988 (Cth), s. 6.

[63] See Australian Privacy Foundation, *Submission to Senate Legal and Constitutional Inquiry into Privacy Act 1988* (March 2005) 7.

[64] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002, *OJ*, L 201, 31 July 2002, p. 0037–0047 ('Directive on Privacy and Electronic Communications').

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information . . . inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.[65]

A 2005 review of the Australian Privacy Act by a Senate Committee recognised that the definition of 'personal information' may need to be extended to deal with new technologies, while recommending that the issue be examined as part of a proposed future review.[66]

In our view, the proper scope of data protection laws should be determined on the basis of whether online privacy is conceived from a 'rights-based' or 'interests-based' perspective. From a 'rights-based' perspective, if information generated by a person online is seen as an expression of the person's identity, there may be a 'rights-based' argument for conferring control over the information to protect the ability of the person to freely develop in the online environment, regardless of whether or not the person can be identified from the information.[67] If online privacy is regarded as an 'interest', however, other interests, including the interest of business in being able to freely process online information, and interests in ensuring the accuracy of information, must be given some weight in determining the scope of data protection laws. In that case, it may well be that the interests of business in contacting individuals will outweigh the interests of individuals in being free from unsolicited online communications.

[65] Transposed into UK law by Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK). The justification for the requirement is set out in Recital 24 to the Directive which provides, in part, that: 'Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms'.

[66] Australia, Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (Canberra: Senate Printing Unit, June 2005), Recommendation 6, paras. 7.14–15. In January 2006, the federal Attorney-General directed the Australian Law Reform Commission (ALRC) to undertake a comprehensive review of Australian privacy law. The ALRC is to report by March 2008. The terms of reference for the review are available at www.alrc.gov.au/inquiries/current/privacy/terms.htm.

[67] This is part of the broader set of issues relating to identity online, sometimes referred to as the 'digital persona' or 'digital identity': see, e.g., Roger Clarke, 'The Digital Persona and its Application to Data Surveillance' (1994) 10(2) *The Information Society*, reproduced at http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html.

Secondly, the difference between 'rights-based' and 'interests-based' approaches to privacy may be illustrated by comparing some of the substantive features of the Data Protection Directive with those of the Australian Commonwealth Privacy Act. Thus, the Australian Act includes a complex array of exceptions and exemptions that are not found in the Data Protection Directive, including important exemptions for small business,[68] expressly aimed at minimising regulatory costs, and for employee records.[69] Direct marketing is also treated more liberally under the Australian Act than under the Data Protection Directive. While the former establishes a general 'opt out' regime for direct marketing,[70] it also allows personal information to be used or disclosed for direct marketing without consent of the data subject where direct marketing is the primary purpose of collecting the information.[71] Article 14(b) of the Directive, in contrast, establishes specific rights for the data subject to object to the processing of personal data for the purposes of direct marketing, and to be informed before personal data are disclosed to third parties for the first time for such purposes. Finally, although both regimes generally allow for personal information to be processed with the consent of the data subject, the formal legal requirements for consent differ. While the Privacy Act allows for consent to be implied,[72] the Data Protection Directive requires that the consent of the data subject must be a 'freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.[73]

Electronic surveillance

In addition to the collection of identifying information, some DRM systems incorporate the ability to monitor, or conduct surveillance of, activities of an end user associated with protected content.[74] There are two main forms of reporting and monitoring that may be part of a DRM

[68] Privacy Act 1988 (Cth), ss. 6C(1), 6D.
[69] Ibid. s. 7B(3).
[70] Ibid. National Privacy Principles 2.1(c).
[71] Ibid. National Privacy Principles 2.1.
[72] Ibid. s. 6 (definition of 'consent').
[73] Data Protection Directive, above n. 41, Art. 2(h).
[74] As the International Working Group on Data Protection in Telecommunications put it: 'Electronic Copyright Management Systems (ECMS) are being devised and offered which could lead to ubiquitous surveillance of users by digital works. Some ECMS are monitoring every single act of reading, listening and viewing on the Internet by individual users thereby collecting highly sensitive information about the data subject concerned': International Working Group on Data Protection in Telecommunications, *Common Position on Privacy and Copyright Management*, adopted at the 27th Meeting of the Working Group on 4–5 May 2000. See also Julie E. Cohen, 'DRM and Privacy' (2003) 18 *Berkeley Technology Law Journal* 575; Julie E. Cohen, 'Normal Discipline in the Age of Crisis' (Draft, 4 August 2004), available at http://www.ssrn.com.

system. First, there is reporting and monitoring that occurs as part of a payment mechanism. For example, the system may be designed to require authentication of a user's identity each time that content is accessed or used. The system may then create a record of the user's interaction with the content, so that the user can be billed in accordance with the use, as specified by the digital rights purchased by the user. Secondly, a DRM system may be designed to report back on the activities of the user that are unrelated to the rights purchased by the user. For example, in *Specht* v. *Netscape Communications Corp.*,[75] software that was made available as a 'plug-in' to the Netscape browser was designed to improve the downloading capability of the browser but, at the same time, recorded every web site visited by the user and relayed the information to Netscape.

Privacy concerns relating to electronic surveillance are distinct from, but related to, information privacy concerns. In its 1983 report, *Privacy*, for example, the Australian Law Reform Commission (ALRC) distinguished between territorial privacy, privacy of the person, information privacy, and communications and surveillance privacy.[76] In doing so, the ALRC noted that breaches of communications and surveillance privacy could, but do not necessarily, involve breaches of the three other aspects of privacy. Information privacy, then, may be regarded as a right to (or interest in) limiting access to the unconstrained collection and processing of personally identifiable information. Surveillance privacy, on the other hand, may be defined as a right to (or interest in) limiting access to unconstrained intentional observation, especially persistent observation, of one's activities by others, in particular where this is accomplished by means of interception or surveillance technologies.[77] Surveillance privacy overlaps with information privacy to the extent that the collection and processing of personal information may amount to the surveillance of the activities, especially the online activities, of the data subject.

[75] 306 F. 3d 17 (2002). This example is cited by Cohen 'Normal Discipline in the Age of Crisis', above n. 74.

[76] Australian Law Reform Commission, *Privacy*, above n. 28, p. 13.

[77] In its 2001 Interim Report on surveillance, the New South Wales Law Reform Commission (NSWLRC), after noting that the term 'surveillance' 'defies precise definition', observed that 'surveillance involves using a surveillance device to monitor, either through listening to, watching, or collecting data (in whatever form) about people, places or objects . . . Surveillance may be directed at a particular target or may be random, but is always a deliberate or intentional act of monitoring conducted for the purpose of acquiring information about the subject of the surveillance': NSWLRC, *Surveillance: An Interim Report*, Report no. 98 (Sydney: NSWLRC, 2001), paras. 2.37–8.

The growth of surveillance practices and technologies has been a controversial feature of contemporary western societies. While privacy concerns arising from surveillance tend to focus on the effects of intrusion on individuals, the potentially ubiquitous surveillance within contemporary information societies has given rise to system-wide concerns. Often cited here is Foucault's well-known discussion of Bentham's design for a model prison, known as the panopticon.[78] The panopticon was designed so that it was possible for individual prisoners to be under observation at any point in time, although the prisoner would not know whether or not this was in fact the case. Social control was therefore maintained through the continual fear of being observed, which eventually ensured that those under observation internalised the desired norms of behaviour.[79] Foucault used the panopticon as a metaphor for the way in which power is exercised in modern societies by 'disciplinary' practices – such as surveillance, documentation and classification – which ensure that people conform to social norms and, indeed, shape what it is to be a person. These practices are associated with an increasing rationalisation of society, as well as a normalisation of individual identities. Wide-spread surveillance can therefore be seen as undermining autonomous decision-making by conditioning people to conform voluntarily to accepted standards of behaviour. As Cohen, for example, has warned: 'Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream.'[80]

Laws regulating surveillance are not as developed as data protection laws. In the past, such laws have mainly been directed at limiting the surveillance practices of government. For example, in the important 1967 decision in *Katz* v. *United States*[81] the US Supreme Court held that electronic monitoring of a telephone call was a 'search and seizure' within the Fourth Amendment, meaning that interception without a warrant did not comply with constitutional standards. In that case, Harlan J pointed out that 'reasonable expectations of privacy may be defeated by electronic as well as physical invasion'.[82] The potential incorporation of surveillance functions in DRM systems, however, creates the increasing possibility of surveillance by non-government actors. Surveillance by DRM systems

[78] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, transl. Alan Sheridan (Harmondsworth: Penguin, 1979) pp. 200–9.

[79] As Foucault put it, the effect is 'to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of the power': ibid. p. 201.

[80] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373 at 1426.

[81] 389 US 347 (1967). [82] Ibid. 362.

must not, therefore, be seen in isolation, but as part of the increasing use of surveillance systems by both public and private sector entities, with possibly worrying consequences for ever more rationalisation and normalisation, and the threat of increased social conformity.[83]

Just as the level of protection afforded by data protection laws differs, depending upon whether the laws are 'rights-based' or 'interests-based', objections to breaches of surveillance privacy may be formulated in either 'rights-based' or 'interests-based' terms. 'Rights-based' objections to surveillance are concerned with the extent to which surveillance, both overt and covert, may undermine individual autonomy and dignity. In relation to overt surveillance, if one knows that one is being watched, then this will clearly influence decisions about the activities one engages in. Covert surveillance, on the other hand, is even more objectionable than overt surveillance. First, it undermines autonomous decision-making because the person under surveillance is unaware of the single most important feature of the situation the person is in: the fact that he or she is being monitored. Such knowledge might obviously lead to the making of different decisions about what that person does. Secondly, by concealing the fact of surveillance, the person under surveillance is denied the respect due him or her as a fellow human being.[84]

At the same time, surveillance may have positive as well as negative consequences.[85] Some degree of surveillance is necessary for the functioning of modern societies, being important for convenience, efficiency and, increasingly, security. The issue is not whether or not there is surveillance, but the appropriate limits to be placed on surveillance technologies and practices. From a 'rights-based' perspective, the degree of surveillance should be strictly proportional to the ends sought to be achieved. This would suggest that DRM surveillance should be as transparent as possible, and limited to that which is necessary to support the interests of content owners. Moreover, in designing DRM systems, the dangers of systematically embedding surveillance systems within everyday life, with the attendant threats of eroding what it is to be a morally autonomous person, should be taken into account.

[83] See, e.g., Sonia K. Katyal, 'The New Surveillance' (2003) 54 *Case Western Reserve Law Review* 297; Cohen, 'Normal Discipline in the Age of Crisis', above n. 74.

[84] For the classic statement outlining deontological objections to covert surveillance see: Stanley I. Benn, 'Privacy, Freedom, and Respect for Persons' in Pennock and Chapman, *Privacy*, above n. 29.

[85] See David Lyon, *Surveillance Society: Monitoring Everyday Life* (Philadelphia: Open University, 2001); David Lyon, 'Everyday Surveillance: Personal Data and Social Classification' (2002) 5(2) *Information, Communication & Society* 242.

From a perspective that regards freedom from surveillance as an 'interest' rather than a 'right', however, concerns at establishing strict limits on surveillance technologies will be less pressing. 'Interests-based' objections to unconstrained surveillance have focused not on the implications of surveillance for moral autonomy, but on the need to avoid socially wasteful expenditure on surveillance technologies and counter-surveillance technologies.[86] This means that 'interests-based' analyses will give more weight to objectives that conflict with the interests of the person subject to surveillance, such as the interests of content owners in efficiently delivering content, and the social interest in minimising enforcement costs. Pure 'interests-based' perspectives are also likely to ignore the potentially negative system-wide effects of the ever more widespread use of surveillance systems.

Self-enforcement mechanisms

As well as providing information about individual users, and about their activities in relation to digital content, DRM systems may directly impose technological controls on what users may, or may not, do with digital content. For example, a particular form of content may be programmed to self-delete after being accessed a certain number of times, or may only be able to be used on particular consumer equipment. The 'broadcast flag' proceedings, before the Federal Communications Commission (FCC) in the United States, was a good example of proposals for DRM systems designed to impose direct restrictions on users.[87] The 'broadcast flag' was aimed at promoting technologies that allowed users to make copies of digital broadcast content for their own purposes, but prevented unrestricted distribution of the content, especially by the internet.[88] Increasingly, it seems that copyright owners are interested in building into consumer electronics some constraints on what users may do with copyright material.

Self-enforcement mechanisms embedded in technology may be distinguished from DRM surveillance technologies in the following way: the

[86] See, e.g., Richard A. Posner, 'The Right to Privacy' (1978) 12 *Georgia Law Review* 293; Richard A. Posner, 'Privacy, Secrecy, and Reputation' (1979) 28 *Buffalo Law Review* 1.

[87] United States, Federal Communications Commission, *In the Matter of Digital Broadcast Content Protection*, Report and Order and Further Notice of Proposed Rulemaking (4 November 2003).

[88] In *American Libraries Association* v. *Federal Communications Commission* (No. 04–1037, decided 6 May 2005), the US Court of Appeals for the District of Columbia Circuit decided that the FCC lacked the authority to impose the 'broadcast flag'.

former impose *ex ante* restrictions on access to, or use of, protected content, whereas the latter are concerned mainly with detecting, and reporting on, activities after they have occurred. In other words, while DRM surveillance technologies involve intrusions on a person's private activities that fall comfortably within our accepted understanding of what it means to invade privacy, the latter do not involve direct intrusions, but may well remove the need for *ex ante* intrusions.

On this point, Cohen has argued that, if surveillance represents an intrusion into privacy, then direct control of a user's activities, which effectively removes the need for intrusion, must be an even greater invasion of privacy.[89] She goes on to claim that technological self-enforcement mechanisms represent an invasion of privacy in two senses in which it has been recognised in the US tradition: as an intrusion into private spaces;[90] and as a breach of the constitutionally recognised right of individuals to make decisions regarding private matters, as first recognised by the Supreme Court in *Griswold* v. *Connecticut*.[91]

This argument raises difficult questions about the meaning of the concept of privacy that are beyond the scope of this chapter. It may be that technological restrictions on what a user may do with digital content should be seen as limiting personal autonomy, in the sense of the capacity of a person to make decisions about his or her 'private' life, rather than as invasions of privacy. In any case, in the same way as invasions of privacy, strictly speaking, may be analysed from either a 'rights-based' or 'interests-based' perspective, so too may restrictions on user autonomy.

If promoting autonomy, meaning the ability of individuals to make decisions for themselves, is regarded as desirable, then widespread use of technological restrictions that dictate how digital content is to be used can be seen as problematic. In other words, technologies may be designed in such a way as to either restrict the ability of users to make decisions about what they can do with the technology, or to maximise user choice. Furthermore, embedding behavioural rules within technology may, like pervasive surveillance, promote greater social conformity over time. From a 'rights-based' perspective, therefore, the pervasive use of DRM self-enforcement technologies might be thought to erode the autonomy and dignity of users of copyright material.

[89] Cohen, 'DRM and Privacy', above n. 74, 582.

[90] On this characteristic feature of the American tradition see Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1161.

[91] 381 US 479 (1965).

From an 'interests-based' perspective, on the other hand, such technological constraints might be seen as useful insofar as they preserve incentives by preventing uncompensated uses of digital material, and reduce enforcement costs for content owners. Furthermore, by helping markets for copyright material to be divided according to individual preferences, technological restrictions may assist price discrimination which, in this context, is usually thought to enhance economic efficiency. Against these considerations, such constraints may pose the danger of content owners extracting uneconomic rents.

To date, there has been no specific regulation of the way in which emerging technologies may restrict what users can do. But there is evidence of support emerging for the idea that the privacy implications of new technologies should be considered at the time at which they are designed or implemented. For example, a 2005 Senate review of Australian privacy laws favoured the introduction of a statutory privacy impact assessment process for new projects that may adversely affect privacy, and proposed that a future review of privacy laws consider the privacy implications of new and emerging technologies to determine whether they are adequately regulated.[92] It appears increasingly apparent that both copyright law and privacy law-making will, in the future, be concerned with the choices made in the design of technologies. Clearly, a 'rights-based' approach to protecting user autonomy will be more concerned about widespread technological constraints on user behaviour, and more favourable to some form of regulation of such technologies, than will an 'interests-based' approach.

Copyright, privacy and DRM

It will be clear that difficult policy issues arise in defining the appropriate relationship between copyright and privacy. The extent to which some form of legal regulation is needed to ensure an appropriate balance in the context of DRM systems is even more difficult. In truth, it is still too early in the development and implementation of these systems for any definitive conclusions to be drawn.

To date, the official policy responses have been limited, with the most detailed examination thus far being undertaken by the European Union

[92] Australia, Senate Committee, *The Real Big Brother*, above n. 66, Recommendations 5 and 8, paras. 7.13 and 7.24. The terms of reference for the ALRC review, referred to at n. 66 above, instruct the ALRC to consider 'the need of individuals for privacy protection in an evolving technological environment'.

within the framework established by the Data Protection Directive. In early 2005, a working document prepared by the Working Party established under Article 29 of that instrument confirmed the application of the EU data protection principles to DRM systems.[93] In particular, the document emphasised the following specific issues:

- the need to preserve anonymous access to network services;
- the desirability of limiting the extent to which a specific individual is linked to a document to circumstances in which it is necessary for the performance of a service or where the individual has consented to the link;
- the importance of establishing the greatest possible transparency in DRM systems, including that users are informed, prior to the collection of personal data, of the identity of the data controller, the purposes of data processing, the recipients of the data and the existence of a right of access and rectification;
- the need to ensure that personal data is used only for the stated purpose of collection and not, for example, for the purpose of direct marketing when the purpose of collection is authentication of payment; and
- the need to ensure that personal data is kept in a form that permits identification of the data subject for no longer than is necessary for the purpose for which the data has been collected.

This analysis is clearly based on a particular perspective, viewing the issues through the lens of the EU 'rights-based' approach to data protection. Other jurisdictions, however, may take a different approach, particularly if they adopt an 'interests-based' analysis. Indeed, the main point made in this chapter is that, to understand properly the relationship between copyright and privacy, an essential starting point is to identify and articulate the perspective from which that relationship is to be analysed. Thus, the appropriate level of copyright protection in the digital environment will differ depending upon whether copyright is predominantly regarded as protecting authors' rights (as in civil law systems), or as supporting markets in copyright material (a more peculiarly common law approach). In the same way, the level of protection accorded privacy will vary depending upon whether this is regarded as a fundamental right that is essential to the autonomy and dignity of persons, or if it is simply regarded as an individual 'interest' (or preference) that is to be balanced

[93] Article 29 Working Party, *Working Document on Data Protection Issues related to Intellectual Property Rights*, WP 104, 18 January 2005.

with other interests, with the final judgment being made on utilitarian grounds.

For example, adopting a predominantly utilitarian, 'interests-based' analysis might mean that a prospective law regulating the use of DRM systems would fall to be assessed by reference to its capacity to promote markets in copyright material. Under such an approach, potentially privacy-invasive measures might be defensible as being necessary for the reduction of transaction and enforcement costs as well as having possible consumer benefits, including the more accurate tracking and targeting of consumer preferences. By contrast, a 'rights-based' analysis that emphasises the protection of the autonomy and dignity of users may justify limitations on the use of such measures, even where those limits could not be justified from a purely economic perspective. Finally, if 'rights-based' arguments for the protection of authors are factored into the analysis, there is the complex task of balancing two, potentially competing sets of rights: the personality rights of authors and the privacy rights of users.

Conclusion

This chapter has argued that, in assessing emerging DRM systems, it is important to distinguish, both historically and conceptually, between the two main western legal traditions for understanding copyright and privacy: a 'rights-based' approach and a utilitarian, 'interests-based' approach. The two approaches reflect quite different views of the relationship between the law and the market. From a 'rights-based' perspective, the role of the law is mainly to establish limits on the market to protect the autonomy and human dignity of both authors and content users. But from a utilitarian/economic perspective, the main role of the law is to support the efficient operation of markets.

At present, it is still far too early in the development of DRM systems to be able to adequately assess such systems from either a 'rights-based' or 'interests-based' perspective. We simply do not have sufficient information about how those systems might work in practice for any sensible conclusions to be drawn.

As these systems are being developed, however, we suggest that it is important to commence a more detailed analysis of some specific issues than has been attempted to date. In our view, the most pressing matters for investigation are:

- the functions or design elements of DRM systems that promote economic efficiency, and those that may undermine efficiency objectives;

- the economic analysis of laws that apply to DRM systems, especially anti-circumvention laws;
- the extent to which it is desirable for copyright laws to promote values other than market-based values, including privacy rights and rights to freedom of expression;
- the extent to which values other than market-based values, especially rights to privacy, should be taken into account in determining the legal framework to apply to DRM systems;
- the adequacy of existing privacy laws, especially data protection laws, for regulating DRM systems, in particular whether these adequately capture all of the privacy implications of DRM systems, or whether they need to be extended to take account of other concerns, such as the potential surveillance of end users; and
- the extent to which the privacy of content users may require the development of specific technical tools, such as Privacy Enhancing Technologies, in addition to legal forms of protection.[94]

In other words, detailed attention is required to examine the appropriate level of control that owners should have over digital content and the extent to which limits on control may be justified in order to protect content users, including their rights to privacy. While the combination of technological developments and the global trade in digital content may well lead to paradigm shifts in legal traditions as they apply to digital content, it is important, at this stage, that the policy choices available for regulating DRM systems be understood. We also consider it important that, in addressing these new and emerging technologies, the values underlying policy decisions are made more transparent than has been the case to date. It is only when this is done that it will be possible for laws to be formulated that appropriately reflect both the important values served by the protection of authors' rights and copyright material, on the one hand, and the protection of end user privacy, on the other.

[94] The importance of technological measures for the protection of privacy has received official acknowledgement. E.g., the Australian Privacy Commissioner's 2005 review of the private sector provisions of the Privacy Act stated that: 'There is a role for technology itself in protecting privacy, often called Privacy Enhancing Technology or PETS. E.g., a system can be built to allow anonymity, or it can be built in a way that identifies every step a user takes': Office of the Privacy Commissioner, *Getting in on the Act*, above n. 60, p. 241.

7

Why there will never be an English common law privacy tort

RAYMOND WACKS

ONCE AGAIN, A FALSE DAWN. Stars linger in the sky, while an expectant band of terrestrial stars – pop stars, sports stars, stars of screen, radio, television, and the catwalk – accepts defeat, their dejection matched only by the misery of their lawyers. Few need be retold the tale of the English common law's failure to recognise, along American lines, a privacy tort (or torts), and I shall not repeat it here. My present purpose is to attempt to explain this unhappy state of affairs. Unhappy, because – despite the celestial image sketched above – the private lives of 'ordinary' individuals are equally vulnerable to unwanted publicity and warrant legal protection.[1]

A common law privacy tort has been long in gestation. For almost four decades, the courts have danced around the problem. Numerous cases involving celebrities have been pleaded, mostly unsuccessfully, in equity as breaches of confidence, and, while the relationship between this remedy and a tort of privacy has been widely acknowledged, the highest court again has been presented with an opportunity to declare what the law is. In

I am most grateful to Megan Richardson, David Lindsay, Andrew Kenyon, Paul Chadwick, and those who attended the seminar at which an earlier version of this chapter was delivered under the auspices and kind hospitality of the Centre for Media and Communications Law in the Faculty of Law at the University of Melbourne on 5 February 2004. Their helpful comments have greatly improved what follows, though the usual disclaimer obtains.

[1] Dissatisfaction with judicial inertia periodically reaches a crescendo; see, e.g., the debate that followed the denial of a remedy to the plaintiff in *Kaye* v. *Robertson* [1991] FSR 62 whose photograph was taken while he was convalescing in a private room of a hospital from which most visitors were explicitly barred. See Basil S. Markesinis, 'Our Patchy Law of Privacy – Time to Do Something About it' (1990) 53 *Modern Law Review* 802; Peter Prescott, '*Kaye* v. *Robertson* – A Reply' (1991) 54 *Modern Law Review* 451; Basil S. Markesinis, 'The Calcutt Report Must Not Be Forgotten' (1992) 55 *Modern Law Review* 118; David Feldman, *Civil Liberties and Human Rights in England and Wales*, (2nd edn, Oxford: Oxford University Press, 2002), Part 3; Gavin Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726.

the interim, the enactment of the Data Protection Act 1998, and especially the Human Rights Act 1998, have served as significant catalysts for a final reckoning.[2] The latter (which came into effect on 2 October 2000) has exercised a considerable influence on the judicial deliberation of privacy issues. The Act incorporates into English law Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) which provides for the protection of the right to respect for family life, home and correspondence.[3] This measure, at least in the mind of one senior judge, gives 'the final impetus to the recognition of a right of privacy in English law'.[4] Though his sanguine view may not be shared by all members of the judiciary, the analysis of privacy exhibited in recent cases suggests that the effect of Article 8 is to supply, at least, the potential for the horizontal application of the rights that it contains.[5]

Though the appellant's 'privacy' was ultimately vindicated, the House of Lords in *Naomi Campbell* v. *MGN* Ltd[6] provided less than clear guidelines on the central question of what constitutes 'private facts' in a case where they have been gratuitously publicised. Indeed, it would be no exaggeration to describe this issue as lying at the heart of the court's 3–2 division. And I shall argue below that until this fundamental problem is satisfactorily resolved, the prospects for a privacy tort of public disclosure of private facts are bleak.

There are, I believe, seven principal factors that combine to explain and foster the notorious judicial inertia in this field and, though the preponderance of my remarks will concern judgments of the courts of England and Wales, the decisions of other jurisdictions, especially Australia and New Zealand, cannot, of course, be ignored. The seven factors are as follows:

1. The advance of the equitable remedy for breach of confidence
2. The impact of the Human Rights Act 1998
3. The dominance of freedom of expression

[2] For a discussion of these early decisions, see Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1993) pp. 82–100, and Raymond Wacks, *Privacy and Press Freedom* (Oxford: Oxford University Press, 1995) chap. 3.

[3] Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952).

[4] *Douglas* v. *Hello! Ltd* [2001] QB 967 at para. 111 (Sedley LJ). Cf. Lord Hoffmann in *Wainwright* v. *Home Office* [2004] 2 AC 406, discussed below n. 20.

[5] Whether such horizontality is a consequence of the Act is left uncertain by the House of Lords in *Campbell* v. *MGN Ltd* [2004] 2 AC 457. This is a subject for another day.

[6] *Campbell* v. *MGN Ltd* [2004] 2 AC 457.

4. The impact of the Data Protection Act 1998
5. Media self-regulation
6. Incoherence of the concept of privacy
7. Judicial preference for legislation

Before these factors cane be explored in detail, the majority decision of the House of Lords in *Naomi Campbell* needs to be understood in the context of the prevailing legal climate that preceded it.

Towards *Naomi*

A decade has, incredibly, passed since I wrote:

> A statutory cause of action for the public disclosure of private facts (subject, of course, to the accepted defences) is the best way forward. But if Parliament is unwilling to grasp the nettle, the courts must. The combined force of three recent developments provide ample support for initiative in an appropriate case: the expanding equitable remedy for breach of confidence, the revived tort of inflicting emotional distress, and the growing influence of the international recognition of 'privacy', especially the jurisprudence of the European Convention on Human Rights. With these weapons to hand, the campaign demands only modest judicial heroism.[7]

The first and last of these developments have, in the last few years, actually engendered what may seem at first to be the mild judicial activism for which I had the temerity to call. The enlargement of the equitable remedy of breach of confidence – spearheaded by bolder judges Down Under – and the adoption in Britain (through the passage of the Human Rights Act 1998) of the European Convention on Human Rights have recently generated a flurry of decisions by the English Court of Appeal and the House of Lords that, though they have won plaudits from privacy advocates, ought perhaps to give us pause to consider whether they reflect judicial courage or confusion.

In *Douglas* v. *Hello! Ltd*,[8] photographs of the wedding of Michael Douglas and Catherine Zeta-Jones were surreptitiously taken, notwithstanding explicit notice having been given to all guests forbidding 'photography or video devices at the ceremony or reception'. The couple had entered into an exclusive publication contract with *OK!* magazine, but its rival, *Hello!*, sought to publish the pictures. The Court of Appeal permitted

[7] Wacks, *Privacy and Press Freedom*, above n. 2, p. 173.
[8] [2001] QB 967, CA; *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996; *Douglas* v. *Hello! Ltd* [2005] HRLR 27.

it to do so, largely on the ground the wedding reception was not an essentially 'private' matter. Indeed, the court was of the view that it had become a commercial transaction. From the point of view of the action for breach of confidence, there was little to support the proposition that the information was indeed 'confidential'. The case, therefore, resembles in some respects what the American courts have called the 'appropriation of name and likeness' – though, oddly, none of the judges in the Court of Appeal mentions this tort. It should also be noted that the court attached considerable importance to the right of freedom of expression, as protected by section 12 of the Human Rights Act 1998.

In the course of his portentous judgment, Sedley LJ announced that the right of privacy had, at last, arrived in England:

> [W]e have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right of personal privacy.[9]

This is the case, he continues, for two reasons: first, because of the growing recognition of a need for 'private space'. Secondly, in order to give effect to the right to 'respect for family life' provided for by Article 8 of the European Convention on Human Rights. Neither of these grounds, it must be said, affords a precise or persuasive argument for 'the confidence' expressed by the learned judge in the recognition of this right. But this is not the place to consider the judgment in detail. Suffice it to say that his analysis of what he rather precipitately calls the 'tort' of breach of confidence leaves several questions unanswered. Moreover, the nebulous equation of 'privacy' and 'the fundamental value of autonomy' merely compounds the woolly contours of a decision which, though it may be supportable in its outcome, provides an unsatisfactorily vague evaluation (by all three members of the Court of Appeal) of the action for breach of confidence and, in particular, its application to the protection of personal information.

The court appears sensibly to have drawn a distinction between what American law calls a 'right to publicity', on the one hand, and a right to privacy, on the other. The former has provided celebrities with the means to assert that by publishing private information about them, the defendant has deprived them of their 'right' to exploit their celebrity status for profit. Restraints on the exercise of freedom of expression would, the court held, be ordered only where 'privacy' properly so-called has been invaded by unwanted publicity.

[9] *Douglas* v. *Hello! Ltd* [2000] QB 967 at para. 110.

In view of the alacrity with which Sedley LJ heralded a new dawn of privacy, it is worth quoting the learned judge at some length. Addressing the role of the law of confidence, Sedley LJ states:

> The courts have done what they can, using such legal tools as were to hand, to stop the more outrageous invasions of individuals' privacy; but they have felt unable to articulate their measures as a discrete principle of law. Nevertheless, we have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right of personal privacy . . . The reasons are twofold. First, equity and the common law are today in a position to respond to an increasingly invasive social environment by affirming that everybody has a right to some private space. Secondly, and in any event, the Human Rights Act 1998 requires the courts of this country to give appropriate effect to the right to respect for private and family life set out in Article 8 of the European Convention on Human Rights and Fundamental Freedoms. The difficulty with the first proposition resides in the common law's perennial need (for the best of reasons, that of legal certainty) to appear not to be doing anything for the first time. The difficulty with the second lies in the word 'appropriate'. But the two sources of law now run in a single channel because, by virtue of section 2 and section 6 of the Act, the courts of this country must not only take into account jurisprudence of both the Commission and the European Court of Human Rights which points to a positive institutional obligation to respect privacy; they must themselves act compatibly with that and the other Convention rights. This, for reasons I now turn to, arguably gives the final impetus to the recognition of a right of privacy in English law.[10]

The learned judge concludes that 'at lowest':

> Mr Tugendhat has a powerfully arguable case to advance at trial that his two first-named clients have a right of privacy which English law will today recognise and, where appropriate, protect. To say this is in my belief to say little, save by way of a label, that our courts have not said already over the years. It is to say, among other things, that the right, grounded as it is in the equitable doctrine of breach of confidence, is not unqualified . . . What a concept of privacy does, however, is accord recognition to the fact that the law has to protect not only those people whose trust has been abused but those who simply find themselves subjected to an unwanted intrusion into their personal lives. The law no longer needs to construct an artificial relationship of confidentiality between intruder and victim: it can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy.[11]

[10] Ibid. paras. 110–11. [11] Ibid. paras. 125–6.

Sedley LJ then turns to section 6 of the Human Rights Act 1998 that provides that the court as a public authority cannot act in a manner incompatible with a Convention right:

> If it is not – for example if the step from confidentiality to privacy is not simply a modern restatement of the scope of a known protection but a legal innovation – then I would accept his submission . . . that this is precisely the kind of incremental change for which the Act is designed: one which without undermining the measure of certainty which is necessary to all law gives substance and effect to section 6.[12]

He adds that, 'Such a process would be consonant with the jurisprudence of the European Court of Human Rights, which section 2 of the Act requires us to take into account and which has pinpointed Article 8 as a locus of the doctrine of positive obligation.'[13]

In the course of his judgment, Keene LJ notes that although the particulars of claim were put in terms of breach of confidence, while it was said in argument for the claimants that the case has more to do with privacy that with confidentiality:

> [I]t is clear that there is no watertight division between the two concepts. *Duchess of Argyll* v. *Duke of Argyll* [1967] Ch 302 was a classic case where the concept of confidentiality was applied so as, in effect, to protect the privacy of communications between a husband and wife. Moreover, breach of confidence is a developing area of the law, the boundaries of which are not immutable, but may change to reflect changes in society, technology and business practice.[14]

Regarding the application of Section 6(1), it:

> . . . arguably includes their activity in interpreting and developing the common law, even where no public authority is a party to the litigation. Whether this extends to creating a new cause of action between private persons and bodies is more controversial, since to do so would appear to circumvent the restrictions on proceedings contained in section 7(1) of the Act and on remedies in section 8(1). But it is unnecessary to determine that issue in these proceedings, where reliance is placed on breach of confidence, an established cause of action, the scope of which may now need to be approached in the light of the obligation on this court arising under section 6(1) of the Act.[15]

[12] Ibid. para. 129. [13] Ibid. para. 130. [14] Ibid. para. 165. [15] Ibid. para. 166.

Citing *Guardian Newspapers (No. 2)*[16] as authority that a pre-existing confidential relationship between the parties is not required for a breach of confidence suit, Keene LJ elaborates:

> The nature of the subject matter or the circumstances of the defendant's activities may suffice in some instances to give rise to liability for breach of confidence. That approach must now be informed by the jurisprudence of the Convention in respect of Article 8. Whether the resulting liability is described as being for breach of confidence or for breach of a right to privacy may be little more than deciding what label is to be attached to the cause of action, but there would seem to be merit in recognising that the original concept of breach of confidence has in this particular category of cases now developed into something different from the commercial and employment relationships with which confidentiality is mainly concerned.[17]

The Court of Appeal unanimously dismissed the appeal of *Hello!* against the judgment in favour of the Douglases based on privacy and commercial confidence, but allowed its appeal against the judgment in favour of *OK!* based on commercial confidences. In acknowledging the right of celebrities to profit from the publication of private information, the court held that private rights in photographs of private occasions subsist even after their commercial sale.

It accepted that notwithstanding the fact that the unauthorised photographs contained the same essentials as the authorised ones (the bride's dress and the wedding cake), they displayed details that the couple wanted to keep private, particularly a photograph of Michael Douglas feeding cake to his new spouse. The court also rejected the earlier decision to lift the interlocutory injunction, banning *Hello!* from publishing the unauthorised photos. It recognised that an injunction was the only viable remedy for a celebrity whose privacy has been infringed, as damages are seldom sufficient.

Following *Von Hannover* v. *Germany*,[18] the court attached considerable importance to the obligation of English courts under the Human Rights Act to protect privacy as provided in Article 8 of the European Convention on Human Rights. And it lamented the difficulty hitherto encountered by courts having to 'shoe-horn' privacy claims into the action for breach of confidence:

[16] *Attorney-General* v. *Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109.
[17] *Douglas* v. *Hello! Ltd* [2000] QB 967 at para. 166. [18] (2005) 40 EHRR 1.

> We conclude that, in so far as private information is concerned, we are required to adopt, as the vehicle for performing such duty as falls on the courts in relation to Convention rights, the cause of action formerly described as breach of confidence. As to the nature of that duty, it seems to us that sections 2, 3, 6 and 12 of the Human Rights Act all point in the same direction. The court should, insofar as it can, develop the action for breach of confidence in such a manner as will give effect to both Article 8 and Article 10 rights. In considering the nature of those rights, account should be taken of the Strasbourg jurisprudence. In particular, when considering what information should be protected as private pursuant to Article 8, it is right to have regard to the decisions of the ECtHR. We cannot pretend that we find it satisfactory to be required to shoe-horn within the cause of action of breach of confidence claims for publication of unauthorised photographs of a private occasion.[19]

The court does not tell us what it *would* find satisfactory, but one is presumably meant to infer that, following *Von Hannover*, the amorphous jurisprudence of the European Court under Article 8 fits the bill.

There is much to digest in the rich diet of these sweeping – sanguine[20] – dicta, but, for the moment, I shall resist the tempting feast, and briefly consider the seven factors that appear to impede the passage towards a full-blown tort of public disclosure of private facts along American lines.

The seven stumbling blocks

In seeking to explain why, in the main, our judges routinely shrink from recognising a common law tort of privacy I suggested above that there are, in no particular order, at least the following seven factors.

[19] *Douglas* v. *Hello! Ltd* [2006] QB 125 at para. 53.

[20] Lord Hoffmann, in both *Campbell* v. *MGN Ltd*, and *Wainwright* v. *Home Office*, firmly declined Sedley LJ's invitation to the privacy party. In *Wainwright* he declared, '[T]he coming into force of the Human Rights Act 1998 weakens the argument for saying that a general tort of invasion of privacy is needed to fill gaps in the existing remedies. Sections 6 and 7 of the Act are in themselves substantial gap fillers; if it is indeed the case that a person's rights under article 8 have been infringed by a public authority, he will have a statutory remedy. The creation of a general tort will, as Buxton LJ pointed out in the Court of Appeal, at [2002] QB 1334, 1360, para. 92, pre-empt the controversial question of the extent, if any, to which the Convention requires the state to provide remedies for invasions of privacy by persons who are not public authorities.'

One: the advance of the equitable remedy for breach of confidence

The equitable remedy for breach of confidence has long been recognised as a means by which personal privacy may be – and has been – protected. Lately, however, the courts have all but treated confidence as synonymous with, or, at least, a surrogate of privacy. Nor is this development confined to English decisions. The High Court of New Zealand recently found that the equitable remedy for breach of confidence (as developed by the English judges) afforded an adequate cause of action for the plaintiff, a celebrity who had been subjected to intrusive photography by the media.[21] The New Zealand Court of Appeal opened the door to the recognition of a full-blown privacy tort,[22] yet the appellants were unable to establish that the tort had been committed. Indeed in both its analysis of the issues and its approach to liability, the Court of Appeal's approach differs little from English boiler-plate breach of confidence cases involving personal information.

Principles of breach of confidence

Before analysing briefly this remarkable evolution, it is perhaps useful to summarise the principal elements of the current legal position. A duty may arise if a person accepts the information on the basis that confidentiality will be maintained, or where a third party receives information from a person who is under a duty of confidence in respect of it and the third party knows, or ought to know, that it has been disclosed to him or her in breach of confidence. Though most cases concern commercial, industrial, or trade secrets, the disclosure of marital confidences or sexual conduct of an individual may be restrained or compensated. The English law has developed in the context of obligations arising under the Human Rights Act 1998 (discussed below). A number of principles may be culled from recent cases.[23]

[21] *Hosking* v. *Runting* [2003] 3 NZLR 285.

[22] *Hosking* v. *Runting* [2005] 1 NZLR 1.

[23] See *A* v. *B plc* [2003] QB 195 at paras. 11(ix) and (x), CA; *Venables* v. *Newsgroup Newspapers Ltd* [2001] 1038 at para. 81; *Theakston* v. *MGN Ltd* [2002] EMLR 22 at paras. 77–80, QB; *Attorney-General* v. *Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109 at 281; *Douglas* v. *Hello! Ltd* [2001] QB 967 at paras. 68–9 and 71, CA, citing *Creation Records Ltd* v. *News Group Newspapers Ltd* [1997] EMLR 444 and *Shelley Films Ltd* v. *Rex Features Ltd* [1994] EMLR 134. This summary is adapted from the report of Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy* (Hong Kong: The Commission, December 2004). The report may be found at www.info.gov.hk/hkreform. I am a member of the Commission's privacy sub-committee that formulated these proposals.

Where there is an intrusion in a situation in which a person can reasonably expect his or her privacy to be respected then that intrusion will be capable of giving rise to liability in an action for breach of confidence unless the intrusion can be justified. The bugging of one's home or the use of other surveillance techniques, such as a long lens, are examples of such an intrusion.

It is unnecessary to show a pre-existing relationship of confidence where private information is involved. A duty of confidence will arise whenever the party subject to the duty is in a situation where they either know or ought to know that the other person can reasonably expect their privacy to be protected. The existence of a relationship such as to create a duty of confidence may, and in personal confidence cases commonly will, have to be inferred from the facts.

An injunction may be granted to restrain the publication of photographs taken surreptitiously in circumstances such that the photographer is to be taken to have known that the occasion was a private one and that the taking of photographs by outsiders was not permitted.

Equity may intervene to prevent the publication of photographic images taken in breach of confidence. If, on some private occasion, the prospective claimant makes it clear, expressly or impliedly, that no photographic images are to be taken of him, then all those who are present will be bound by the obligation of confidence created by their knowledge (or imputed knowledge) of that restriction.

The action for breach of confidence seeks to preserve confidentiality and the trust that the plaintiff has reposed in the confidant; it does not endeavour to protect individuals from emotional distress and embarrassment caused by an infringement of their privacy. A number of difficulties therefore arise when a plaintiff relies on this action to afford a remedy for unwarranted infringement of privacy.

Limits on application of breach of confidence to privacy concerns

The following problems offer some indication of the limits of the action in a privacy setting.

The courts have not established clear criteria for determining what kinds of personal information have the necessary quality of confidence about them, other than the negative requirement that the information must not be in the public domain. So for example, the law does not impose an obligation of confidence merely because the information relates to an individual's private or sexual life.

The concept of a relationship of confidentiality may well be inapplicable to transitory or commercial sexual relationships even though information relating to sexuality engages an intimate aspect of private life requiring special protection. Thus, where the parties are not married and one of them informs the media about their sexual relationship without the consent of the other party, the fact that the confidence was a shared confidence which only one of the parties wishes to preserve would undermine the other party's right to have the confidence respected. Extra-marital sexual relations would therefore lie 'at the outer limits of relationships that require the protection of the law'.[24] *A fortiori*, when the relationship is one between a prostitute in a brothel and her client. The fact that they participate in sexual activity does not of itself constitute a sufficient basis for the attribution of confidentiality to the relationship. Such a relationship has therefore been held to be not confidential, even though the latter was keen to keep it secret. Thus, although the courts appear to have eliminated the requirement of a pre-existing relationship, the fact that only one party wishes to keep the information private and confidential deprived the plaintiffs in *A* v. *B plc* and *Theakston* v. *MGN Ltd* of the protection under the law of confidence. The requirement of an agreement to keep the information confidential therefore renders actions for breach of confidence inadequate for the purposes of protecting an individual against invasion of privacy by unwanted publicity.[25]

Certain private information that is in the public domain may nevertheless warrant protection from further disclosure. Images of a private individual in a public place taken without their knowledge and consent may relate to and affect his or her private life, particularly when accompanied by a story revealing details of that private life. In *Peck* v. *UK*[26] the applicant was filmed by a local authority CCTV (Closed Circuit Television) in a public street, brandishing a knife with which he had attempted to commit suicide. The authority later disclosed to the media the footage as well as still pictures, resulting in the applicant's images being published and broadcast. The British government suggested that the applicant would have been entitled to bring an action for breach of confidence if he had been filmed 'in circumstances giving rise to an expectation of privacy on his part'. But the European Court of Human Rights held that the applicant

[24] *A* v. *B plc* [2003] QB 195 at paras. 11(xi), 43(iii) and 47.

[25] *Theakston* v. *MGN Ltd* [2002] EMLR 22 at paras. 57–64 and 72–6, QB endorsed by the Court of Appeal in *A* v. *B plc*, ibid.

[26] (2003) 36 EHRR 41. See Phillipson, 'Transforming Breach of Confidence?', above n. 1, 744–8 and 757–8.

did not have an actionable remedy in breach of confidence and had no effective remedy before a United Kingdom court in relation to the disclosures by the local authority. The European Court was not persuaded by the government's argument that a finding that the applicant had an 'expectation of privacy' would mean that the elements of the breach of confidence action were established. It was unlikely that the UK courts would have accepted that the images had the 'necessary quality of confidence' about them, or that the information was 'imparted in circumstances importing an obligation of confidence'.

It does not follow from the fact that the information is obtained as a result of unlawful activities that its publication should necessarily be restrained by injunction on the ground of breach of confidence, though this could well be a persuasive consideration when it comes to exercising discretion, a matter I discuss below.

A person who acquires personal information in relation to another without notice of its confidential character (as when the information is not confidential by its nature) may disclose the information even though there is an agreement to keep it secret between the confider and the confidant.

The requirement that the information must have been imparted in circumstances importing an obligation of confidence is problematic where the information was disclosed by a newspaper. The defendant would have to show that the newspaper had been put on notice prior to publication that the disclosure amounted to a breach of confidence owed by the source to the subject of the information. Accordingly, the defendant would have to show that the newspaper had the requisite notice both of the source's duty of confidence and of the source's breach of that duty. Such a duty will not exist in the majority of cases of media intrusion. Even if a duty of confidence exists in the particular case, it is difficult to prove because of the protection afforded to the media regarding their sources and the fact that information will frequently be provided to the media anonymously.

There is no jurisdiction to grant an injunction in respect of personal information already published. Once the information in question is in the public domain, its republication is not actionable as a breach of confidence. The obligation of confidence is discharged once the subject matter of the obligation has been destroyed, even though the destruction was the result of a wrongful act committed by the person under the obligation.[27] But private facts or photographs of an individual which have already been

[27] *A* v. *B plc* [2003] QB 195 at para. 11(x); citing *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199.

published in breach of their privacy may, on republication, cause them further distress, embarrassment and frustration.

Finally, the law of breach of confidence is solely concerned with unauthorised disclosures. It offers no relief when the infringement does not involve, or result in, a disclosure. An intrusion into private premises or surveillance using an aural or visual device is probably not actionable as a breach of confidence.

Naomi Campbell v. *Mirror Group Newspapers*

The class of confidential information, and therefore the reach of the action appears to be expanding to reflect the range of activities undertaken by the rich and famous, though not always with obvious consistency. Thus, the majority of the House of Lords held that the details of Naomi Campbell's attendance at Narcotics Anonymous (NA) was private information which imported a duty of confidence. This was based largely on the view that a breach of confidence had occurred which could not be justified in the public interest (see below.) On the other hand, details of the sexual infidelities of a well-known footballer,[28] and the activities of a famous TV presenter in a brothel[29] either fell short of the required 'confidential' nature of the information, or their disclosure was found to be in the public interest. Thus in *Theakston* v. *MGN Ltd* Ouseley J declared:

> I do not consider it likely that the nature or detail of the sexual activities engaged in within the brothel are confidential. They are activities with a number of prostitutes in return for promises of payment in a brothel accessible to anyone with the money and the inclination. There is nothing about the activity, the participants or the location beyond the mere fact that the activities were of a sexual nature to warrant the imposition of confidentiality.[30]

In *Naomi Campbell* v. *MGN Ltd*,[31] the House of Lords held that the supermodel was entitled to damages and compensation for the publication by the *Daily Mirror* of articles and photographs concerning the fact that she was receiving treatment by NA for her drug addiction. Campbell had publicly denied that she was addicted to drugs, and the Court of Appeal had held that by mendaciously asserting to the media that she did not take drugs, she had rendered it legitimate for the media to put the record straight. Phillips LJ stated:

[28] *A* v. *B plc* [2003] QB 195. [29] *Theakston* v. *MGN Ltd* [2002] EMLR 22, QB.
[30] Ibid. [31] [2004] 2 AC 457.

> We do not consider that a reasonable person of ordinary sensibilities, on reading that Miss Campbell was a drug addict, would find it highly offensive, or even offensive that the *Mirror* also disclosed that she was attending meetings of Narcotics Anonymous. The reader might have found it offensive that what were obviously covert photographs had been taken of her, but that, of itself, is not relied upon as ground for legal complaint.
> [I]t is not obvious to us that the peripheral disclosure of Miss Campbell's attendance at Narcotics Anonymous was, in its context, of sufficient significance to shock the conscience and justify the intervention of the court. On the contrary, we have concluded that it was not.[32]

Since the disclosure of this confidential information was in the public interest, the court took the view that a journalist must be given 'reasonable latitude as to the manner in which that information is conveyed to the public'.[33] If not, the Article 10 right to freedom of expression would be unnecessarily inhibited.

The Court of Appeal expressed also certain fairly expansive opinions upon the relationship between 'privacy' and breach of confidence, and between the latter and the Data Protection Act 1998. In respect of the first, it stated that the development of the law of confidence since the Human Rights Act 1998 came into force has seen information described as 'confidential' not only where it has been confided by one person to another, but where it relates to an aspect of an individual's private life which he does not choose to make public. It considered that the unjustifiable publication of such information would better be described as 'breach of privacy' rather than 'breach of confidence'.[34] The House of Lords demonstrated a similar alacrity to dissolve the distinction between confidence and privacy. Thus Lord Nicholls declares:

> This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship. In doing so it has changed its nature. In this country this development was recognised clearly in the judgment of Lord Goff of Chieveley in *Attorney-General* v. *Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 281. Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in

[32] *Campbell* v. *MGN Ltd* [2003] QB 633 at para. 54.
[33] Ibid. para. 62.
[34] *Campbell* v. *MGN Ltd* [2003] QB 633 (Phillips LJ).

> ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.[35]

It is not entirely surprising that, since the adoption of the Human Rights Act in 1998, the courts should now be content to oversee the withering away of the distinction between 'privacy' and 'confidence'. But this appears to reflect less the development of the law than the spate of recent cases involving unwanted publicity. It may seem unduly doctrinaire to insist on a clearer analytical differentiation between the causes of action.[36] However, the court also lost the opportunity to consider first, given the equitable nature of the remedy for breach of confidence, whether Campbell ought to have come to equity with clean hands, or, on the other hand, the defence that 'there is no confidence in iniquity'. The result reflects, I like to believe, the apparent acceptance of the position for which I essayed all those years ago. But sadly the court's reasoning is not accompanied by a discussion of the leading cases on breach of confidential, personal information steeped in the notion of conscience that has afforded the very means by which the remedy has been widened – particularly in respect of third-party rights, and the development of an objective standard of liability.

There is another disquieting feature of the decision. Both the Court of Appeal and the House of Lords attach considerable importance to the fact that the press has the right to 'put the record straight'. Since Campbell lied about her drug addiction, there is, they held, a public interest in the press revealing the truth. It is difficult to accept this view, and I give this matter further attention when I consider below the incoherence that surrounds the notion of privacy.

Two: the impact of the Human Rights Act 1998

As already observed, the Human Rights Act 1998 incorporates into English law Article 8 of the European Convention on Human Rights which provides for the protection of the right to respect for family life, home and correspondence, and one senior judge has, as a result, suggested that this gives 'the final impetus to the recognition of a right of privacy in English

[35] Ibid. para. 14.

[36] E.g., the equitable remedy differs from any putative 'privacy tort' in respect, e.g., of both who may sue and who may be sued.

law'.[37] (I have above quoted other extracts from the judgment of Sedley LJ in *Hello!*) Though his confident view may not be shared by other judges, recent case law analysis suggests at least the potential for the horizontal application of the right.[38]

For the moment, this appears to consist in judges satisfying themselves that the essentials of Article 8 are met by the law of confidence, but this is unlikely to foreclose wider consideration of the concept of privacy (and its relation to other apparently competing rights) in the future. In any event, it is not unreasonable to apprehend in several of these recent judgments a willingness to allow Article 8 to thwart the conception of a full-blown privacy tort. Occasionally one can almost hear the clang of the sword being replaced in its scabbard.

This resistance is most keenly evident when Article 10 of the European Convention on Human Rights is invoked. I consider this vexed matter below.

Three: the dominance of freedom of speech

It is not, I hope, uncharitable to assert that when addressing the inescapable contest between privacy and free speech, the courts have not always acquitted themselves with great distinction. Freedom of speech is by no means a simple matter.[39] Broadly speaking, justifications for free speech are either consequentialist or rights-based. The former normally draws on the arguments of Milton and Mill (from truth or democracy), while the latter conceives of speech as an integral part of an individual's right to self-fulfilment. When it comes to defending free speech these arguments tend invariably to be amalgamated, and even confused. So, for example, Thomas Emerson discerns four primary justifications which include both sorts of claim: individual self-fulfilment, attainment of the truth, securing the participation by members of society in social, including political, decision-making, and providing

[37] *Douglas* v. *Hello! Ltd* [2000] QB 967 at para. 111 (Sedley LJ).

[38] This is not to suggest that it will portend a tide of Strasbourg Article 8 jurisprudence engulfing English courts, but there is an inescapable judicial recognition that, at its lowest, adherence to the spirit of the Article is required.

[39] See, in particular, Frederick Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge: Cambridge University Press, 1982); and Frederick Schauer, 'Reflections on the Value of Truth' (1991) 41 *Case Western Reserve Law Review* 699. See too Eric Barendt, *Freedom of Speech* (2nd edn, Oxford: Oxford University Press, 2005).

the means of maintaining the balance between stability and change in society.[40]

Supporters of 'privacy', on the other hand, rely almost exclusively on rights-based arguments. Thus, in his classic exposition, Alan Westin suggests that a right of privacy is essential to protect personal autonomy, allowing us to be free from manipulation or domination by others, permit emotional release, afford an opportunity for self-evaluation, and allow limited and protected communication to share confidences and to set the boundaries of mental disturbance.[41]

Problems instantly loom. The extent to which the law may legitimately curtail speech that undermines an individual's 'privacy' is frequently represented as a bout between two bruisers, with free speech inevitably the heavyweight. But the contest may, in fact, amount to mere shadow boxing, for often 'the law of privacy and the law sustaining a free press do not contradict each other. On the contrary, they are mutually supportive, in that both are vital features of the basic system of individual rights.'[42] This claim demands appropriate theoretical justification. In particular, the precise relationship between these competing rights and the 'basic system' is far from uncontentious. Tempting though it is, joining issue here would detract from the main purpose of this chapter.

In the United States the issue of press freedom is of course debated against the backdrop of the First Amendment's injunction that 'Congress shall make no law . . . abridging the freedom of speech, or of the press.' And there are now signs that, under the unfolding sway of the European Convention on Human Rights, English courts are embracing a more expansive interpretation understanding of this liberty.

It is hardly surprising that in their analysis of the relationship between freedom of speech and 'privacy', both courts and commentators employ the latter concept with little consistency. As I have already mentioned, my

[40] Thomas I. Emerson, 'The Right of Privacy and Freedom of the Press' (1979) 14 *Harvard Civil Rights-Civil Liberties Law Review* 329 at 331, reproduced in Raymond Wacks, *Privacy* (Aldershot: Dartmouth; New York: New York University Press, 1993), Volume I at p. 377. See too: Joseph Raz, 'Free Expression and Personal Identification' (1991) 2 *Oxford Journal of Legal Studies* 303; Thomas I. Emerson, 'Towards a General Theory of the First Amendment' (1963) 72 *Yale Law Journal* 877; Ronald Dworkin, 'Censorship and a Free Press' in Part 6 of *A Matter of Principle* (Cambridge, Mass.: Harvard University Press, 1985) pp. 335–87; Ruth Gavison, 'Too Early for a Requiem: Warren and Brandeis were Right on Privacy vs Free Speech' (1992) 43 *South Carolina Law Review* 437; Stanley Fish, *There's No Such Thing As Free Speech* (Oxford: Oxford University Press, 1994); and Feldman, *Civil Liberties and Human Rights*, above n. 1, pp. 580–632.

[41] See Alan Westin, *Privacy and Freedom* (London: Bodley Head, 1967) p. 339.

[42] Emerson, 'The Right of Privacy', above n. 40, 331.

own view is that at the heart of the concern about 'privacy' lies the use or abuse of personal information about an individual. And that by confining the analysis of this and other issues to the control over such personal information, a more coherent means of reconciling the competing values might be found.[43] Attempting to untangle the analytical muddle is beyond the scope of this chapter. I have attempted to uncover its chief features elsewhere.[44]

It is not only in the United States that free speech is frequently a trump card. English judges periodically recognise the importance of freedom of speech and of the press. I have already cited above Lord Hoffmann's Dworkinian pronouncement. There can be little doubt that free speech triumphs, especially when supplemented by an expansive notion of 'public interest' and compounded by occasionally convoluted analogies, especially in England, that, in the absence of the explicit judicial recognition of a right to privacy, seek protection in a wide range of actions in tort and equity.

Nor has this stance significantly shifted since the enactment of the Human Rights Act. Thus in *Venables* v. *News Group Newspapers*[45] the court unequivocally asserted the priority of Article 10, treating 'privacy' as, in effect, an *exception* to Article 10, rather than as expressing a free-standing right.[46] This invariably leads to the annihilation of the plaintiff's right to a private life. It must be the case that the matter ought to be treated with greater refinement. The blunderbuss of 'public interest' all too easily demolishes individual privacy.[47]

Nevertheless, privacy did triumph by a majority in the House of Lords in *Naomi Campbell*. The court was, however, unanimous in acknowledging that in respect of Article 8 (privacy) and Article 10 (free speech) of the European Convention on Human Rights, there was no question of either having precedence over the other.[48] Both rights were to be balanced

[43] For the full argument, see: Wacks, *Personal Information*, above n. 2, pp. 7–30; and Raymond Wacks, 'The Poverty of "Privacy"' (1980) 96 *Law Quarterly Review* 73.

[44] See Wacks, *Privacy and Press Freedom*, above n. 2.

[45] [2001] 1 All ER 908.

[46] Similar lop-sidedness is exhibited in *Mills* v. *News Group Newspapers* [2001] EMLR 41, and *Theakston* v. *Mirror Group Newspapers* [2002] EMLR 22. Cf. *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996 (Lindsay J).

[47] Even in the case of royalty. See the decision of the European Court of Human Rights, upholding the privacy of Princess Caroline of Monaco: *Von Hannover* v. *Germany* (2005) 40 EHRR 1.

[48] [2004] 2 AC 457 at para. 12 (Lord Nicholls), para. 55 (Lord Hoffmann), para. 113 (Lord Hope), para. 138 (Baroness Hale) and para. 167 (Lord Carswell).

against each other at this second stage of the enquiry, and among the considerations that entered into this process were, on the one hand, the duty of the media 'to impart information and ideas of public interest which the public has a right to receive' and the need for the court 'to leave it to journalists to decide what material needs to be reproduced to ensure credibility',[49] and, on the other, the potential of the unauthorised disclosure or publication of the information 'to cause harm' to the claimant.[50]

Lord Hope added that in implementing this balancing exercise

> the right of the public to receive information about the details of [Campbell's] treatment was of a much lower order than the undoubted right to know that she was misleading the public when she said that she did not take drugs . . . [T]he more intimate the aspects of private life which are being interfered with, the more serious must be the reasons for doing so before the interference can be legitimate.[51]

The key factor was that the disclosure of the details of Campbell's treatment at NA, especially the publication of the photographs had the potential to cause harm to her (by, for example, obstructing her efforts to conquer her addiction, by causing her substantial distress). The risk of harm was the principal factor that determined the majority view that her Article 8 right to privacy had been violated by the newspaper.[52]

Lords Hoffmann and Nicholls were unpersuaded by this argument, and held that Article 10 trumped the applicant's privacy claim, Lord Hoffmann pointing to the 'practical exigencies of journalism' which required that editorial decisions 'be made quickly and with less information than is available to a court which afterwards reviews the matter at leisure'.[53]

This is not the place to challenge – again – the failure of courts to distinguish the various categories of speech, let alone the circumstances under, and manner in, which the right is exercised. The consequences of their treatment of speech in a monolithic, undifferentiated manner inevitably generates an unacceptable conflation between gossip and politically relevant publications.[54] I have long argued that in attempting to 'balance' the plaintiff's claim to freedom from public disclosure, on the one hand, against the defendant's claim to exercise freedom of expression, on the other, a number of factors ought to be taken into account, including the defendant's motives and beliefs, the timing of the disclosure, the recipient

[49] Ibid. para. 116 (Lord Hope). [50] Ibid. para. 118 (Lord Hope). [51] Ibid. para. 117.
[52] Ibid. para. 119 (Lord Hope), para. 157 (Baroness Hale), para. 169 (Lord Carswell).
[53] Ibid. para. 62.
[54] This is evident in, e.g., *Theakston* v. *MGN* [2002] EMLR 22 and *A* v. *B plc* [2003] QB 195.

of the disclosure and the burden and standard of proof. Moreover, the volatile concept of 'public interest' should itself be subjected to a careful scrutiny. I have proposed the following tests:

(a) To whom was the information given?
(b) Is the plaintiff a 'public figure'?
(c) Was the plaintiff in a public place?
(d) Is the information in the public domain?
(e) Did the plaintiff consent to the publication?
(f) How was the information acquired?
(g) Was it essential for the plaintiff's identity to be revealed?
(h) How serious was the invasion of the plaintiff's privacy?[55]

Yet the importance of these considerations often appears to be lost on the judges whose zealous equation of privacy and confidentiality, and their eager proclivity to favour free speech (with little explication of its purpose) generally eclipse the need for the careful investigation of such questions.[56]

Four: the impact of the Data Protection Act 1998

It would be an overstatement to claim that the existence of the Data Protection Act 1998 has exerted so strong an influence on English judges that they are satisfied that data protection affords a congenial means of protecting privacy and, therefore, to constitute a barrier against the creation of a common law privacy tort. Nevertheless it seems clear from a number of recent decisions that the provisions of the legislation are (understandably)[57] assimilating privacy questions – especially where the plaintiff complains of unauthorised photography. So, for example, in *Campbell* v. *MGN Ltd*,[58] the Court of Appeal provides a lengthy excursus on the relationship between privacy and the Data Protection Act 1998, section 32 of which provides, in effect, a defence of public interest which, the newspaper argued, must extend to its conduct. The alternative, it sought to show, was that in the absence of the consent of the data subject, a newspaper would

[55] Raymond Wacks, *The Protection of Privacy* (London: Sweet & Maxwell, 1980), pp. 98–106; Wacks, *Privacy and Press Freedom*, above n. 2, pp. 105–12.
[56] See *A* v. *B plc* [2003] QB 195.
[57] This is, I have argued, is not necessarily a bad thing. See, e.g., Raymond Wacks, 'Is the Private Domain Doomed?' in Raymond Wacks, *Law, Morality, and the Private Domain* (Hong Kong: Hong Kong University Press, 2000), chap. 12.
[58] [2003] QB 633. This aspect of the applicant's claim was not pursued in the House of Lords.

hardly ever be entitled to publish any of the information categorised as sensitive without running the risk of having to pay compensation. This is because it would be difficult to establish that the conditions for *processing* any personal information were satisfied.

If this interpretation were correct, the court held, the Data Protection Act 1998 would have created a law of privacy and achieved a fundamental enhancement of Article 8 rights, at the expense of Article 10 rights, extending into all areas of media activity, to the extent that the Act was incompatible with the Human Rights Convention.

The court rejected this view and held:

> [W]e conclude that, where the data controller is responsible for the publication of hard copies that reproduce data that has previously been processed by means of equipment operating automatically, the publication forms part of the processing and falls within the scope of the Act.[59]

I shall not pursue this somewhat byzantine argument though it does, I think, demonstrate the increasing application of data protection legislation in the privacy arena. It should be noted (and this is a subject for another paper) that, in at least three respects, it raises complex legal and practical issues. First it touches on the thorny question of the relationship between the collection (say, by surreptitious photography) and the use (its publication) of personal data. Secondly it raises the no less intractable problem of the distinction, if any, between personal data contained in text, and those that appear in a photograph. And, thirdly, it concerns the difficult issue of the gratuitous photography of individuals in a public place – and their possible publication.

Five: media self-regulation

Media or press councils of various kinds exist in numerous jurisdictions, created by statute in at least fourteen of them. In the United Kingdom three such bodies exist. There is the non-statutory British Press Complaints Commission (PCC). In addition, to regulate various aspects of radio and television broadcasting, the Broadcasting Standards Commission and the Independent Television Commission were established by statute – now subsumed within Ofcom. It would not be unjust to describe the performance of the PCC as disappointing (and I shall not repeat the manifold criticisms – including my own – that have been levelled against

[59] *Campbell* v. *MGN Ltd* [2003] QB 633.

its constitution and operation). The sole importance of the PCC in the present context resides in the fact that Section 12(4) of the Human Rights Act 1998 requires a court when considering cases affecting freedom of expression, to have particular regard, inter alia, to 'any relevant privacy code'.

In a number of recent decisions (including *Hello!*) judges have indeed accepted – occasionally with an almost audible sigh of relief – that the PCC's code affords a workmanlike formula by which to strike a balance between privacy and free speech.[60] The precise relationship between the exercise of judicial and self-regulatory jurisdictions in this sphere has yet to be resolved (probably by judicial review of an adjudication by the PCC), but there is little doubt that courts will continue, as they are bound to do, to resort to the broad terms of clause 3 of the code in cases involving media intrusion. And this deference constitutes yet another hindrance to the recognition of a free-standing privacy tort.

Six: incoherence of the concept of privacy

The legal discourse on 'privacy' is anything but lucid, though it is perhaps tendentious for one who has long regarded this development with unease so to characterise it. Yet while it is undeniable that the concept has expanded considerably since its original formulation by Warren and Brandeis[61] as a right against embarrassing publicity – my focus in this chapter – some may want to repudiate my position that the voluminous literature on the subject has failed to produce a coherent or consistent meaning of a notion which, particularly in the US, continues to provide a forum for contesting, inter alia, the rights of women[62] (especially in respect

[60] The code can be viewed at www.pcc.org.uk/cop/cop.asp.

[61] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193. For examinations of the development of their (fairly limited) tort, see Robert C. Post, 'Rereading Warren and Brandeis: Privacy, Property, and Appropriation' (1991) 41 *Case Western Reserve Law Review* 647; Sheldon W. Halpern, 'The "Inviolate Personality" – Warren and Brandeis After One Hundred Years' (1990) *10 Northern Illinois University Law Review* 387. Some of this section is culled from my introduction in Raymond Wacks (ed.), *Privacy*, above n. 40.

[62] See Martha A. Fineman, 'Intimacy Outside of the Natural Family' (1991) 23 *Connecticut Law Review* 955; Elizabeth Schneider, 'The Violence of Privacy' (1991) 23 *Connecticut Law Review* 973; Anita L. Allen and Erin Mack, 'How Privacy Got Its Gender' (1990) 10 *Northern Illinois University Law Review* 441. See generally, Catharine MacKinnon, *Towards a Feminist Theory of the State* (Cambridge, Mass.: Harvard University Press, 1989).

of abortion),[63] the use of contraceptives,[64] the freedom of homosexuals and lesbians,[65] the right to obscene or pornographic publications,[66] the problems generated by AIDS.[67]

A similar approach is unfolding in other common law jurisdictions. Thus the House of Lords recently accepted – without hesitation – that 'privacy' was in issue where the plaintiff complains of an attack on his or her bodily integrity.[68] On the other hand, Gleeson CJ, exercised greater circumspection (and, in my view, wisdom) when he stated in *Lenah Game Meats*: '[T]he lack of precision of the concept of privacy is a reason for caution in declaring a new tort of the kind for which the respondent contends.'[69]

An important consequence of this harnessing of 'privacy' in the pursuit of so many disparate, sometimes competing, political and social ideals has been inevitable analytical turmoil. It should also be noted that, while this paper is confined to an analysis of what in American law is known as the 'public disclosure of private facts', the confusion that attends all

[63] The Supreme Court's decision in *Planned Parenthood* v. *Casey* 112 S. Ct 2791 (1992) to affirm its judgment in *Roe* v. *Wade* 410 US 113 (1973) plainly reflects a fundamental division in American society on the question of abortion. Justice Scalia's scathing assault on the majority judgment bears ample testimony to the strength of feelings on the issue. See John Hart Ely, 'The Wages of Crying Wolf: A Comment on *Roe* v. *Wade*' (1973) 82 *Yale Law Journal* 920; Robert G. Morgan, '*Roe* v. *Wade* and the Lesson of the *Pre-Roe* Case Law' (1979) 77 *Michigan Law Review* 1724 and Thomas Huff, 'Thinking Clearly about Privacy' (1980) 55 *Washington Law Review* 777.

[64] Following the Supreme Court's decision in *Griswold* v. *Connecticut* 381 US 479 (1965). See Stephen J. Schnably, 'Beyond Griswold: Foucauldian and Republican Approaches to Privacy' (1991) 23 *Connecticut Law Review* 861.

[65] Annamay T. Sheppard, 'Thoughts on *Bowers* v. *Hardwick*' (1988) 40 *Rutgers Law Journal* 521. Frank Michelman develops a 'republican, anti-authoritarian' case and Rubenfeld constructs an 'anti-totalitarian' argument to refute the majority's judgment. See Frank Michelman, 'Law's Republic' (1988) 97 *Yale Law Journal* 1493; Jed Rubenfeld, 'The Right of Privacy' (1989) 102 *Harvard Law Review* 737. See too Kendall Thomas, 'Beyond the Privacy Principle' (1992) 92 *Columbia Law Review* 1431. For Thomas neither of these positions is able to 'yield a sufficiently concrete understanding of the political practices that intersect the law of homosexuality', at 1498. Thomas acknowledges that the concept of 'privacy' provides an inadequate basis on which to protect the rights of the homosexual and lesbian community against homophobic violence.

[66] See *Stanley* v. *Georgia*, 394 US 557 (1969).

[67] See Emily Campbell, 'Mandatory AIDS Testing and Privacy: A Psycholegal Perspective' (1990) 66 *North Dakota Law Review* 449; Richard Turkington, 'Confidentiality Policy for HIV-Related Information: An Analytic Framework for Sorting Out Hard and Easy Cases' (1989) 34 *Villanova Law Review* 871; Raymond Wacks, 'Controlling AIDS: Some Legal Issues' (1988) 138 *New Law Journal* 254 and 283.

[68] *Wainwright* v. *Home Office* [2004] 2 AC 406, HL.

[69] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199.

discussions of the right of privacy is compounded by the existence of three other torts in the American law ('intrusion upon the plaintiff's seclusion or solitude, or into the plaintiff's private affairs', 'publicity which places the plaintiff in a false light in the public eye', and 'appropriation, for the defendant's advantage, of the plaintiff's name or likeness'). I have argued elsewhere that it is only 'public disclosure' and 'intrusion' that are properly comprehended as privacy related wrongs.[70]

While the drawing of the public/private boundary is logically anterior to any conception of the role of the law, it is also constituted by the law. This circularity is compounded by the fact that non-legal regulation of what is apparently 'private' may exercise significant controls over such behaviour. Moreover, it would be misleading to assume that, even in liberal thought, there is a consistent or definitive boundary between what is 'private' and what is 'public'. A vast literature devoted to the resolution of these difficulties inevitably raises complex methodological and epistemological questions that frequently obscure rather than illuminate. In an effort to elucidate the essential nature of 'privacy', I have argued that a more constructive means of resolving some of the problems encountered in regulating the collection, storage and use of private facts about an individual might be found by seeking to identify what *specific interests* of the individual we think the law ought to protect. At the core of the preoccupation with the 'right to privacy' is protection against the misuse of personal, sensitive information.

This is not to deny the importance of rights or even their formulation in broad terms that facilitate their recognition by the common law. But by attempting to address the problem of 'privacy' as the protection of 'personal information', the pervasive difficulties that are generally (and, I believe, mistakenly) forced into the straitjacket of 'privacy' might find a less artificial and more effective legal resolution. The practical consequences of this uncertainty is evident in the House of Lords' failure in *Naomi Campbell* v. *MGN Ltd*[71] to define with adequate precision the central concept of 'private facts'. As mentioned above, the court found in favour of the supermodel. She had publicly denied that she was addicted to drugs, and she had rendered it legitimate for the media to put the record straight. The House of Lords nevertheless held that she was entitled to compensation.

The judgments reveal several perspectives of the emerging tort, particularly in the developing environment of Article 8 of the Human Rights

[70] Wacks, *Personal Information*, above n. 2. [71] [2004] 2 AC 457.

Act. The majority regarded the disclosure of Campbell's attendance at a NA meeting, along with the publication of the images of her leaving the meeting, as intimate medical information that warranted protection, notwithstanding Article 10's protection of speech provision. The view of the minority, on the other hand, was that this information did not amount to sensitive health data, and that some latitude needed to be given.[72]

The court recognises that the claim is based solely on the *publication* of the images, not the intrusive photography by which they were obtained. Thus, Lord Nicholls declares:

> In the case of individuals this tort, however labelled, affords respect for one aspect of an individual's privacy. That is the value underlying this cause of action. An individual's privacy can be invaded in ways not involving publication of information. Strip-searches are an example. The extent to which the common law as developed thus far in this country protects other forms of invasion of privacy is not a matter arising in the present case. It does not arise because, although pleaded more widely, Miss Campbell's common law claim was throughout presented in court exclusively on the basis of breach of confidence, that is, the wrongful *publication* by the 'Mirror' of private *information*.[73]

'Private facts'

There is, as I have pointed out, no clear consensus among the judges in *Campbell* on the critical question of what constitutes 'private information'. Lord Nicholls expresses a strong preference for a test based on whether in regard to the disclosed facts 'the person in question had a reasonable expectation of privacy'.[74] The learned judge explicitly rejects Gleeson CJ's formulation in *Australian Broadcasting Corporation* v. *Lenah Game Meats* that asks whether the disclosure 'would be highly offensive to a reasonable person'.[75] This test, according to Lord Nicholls, is stricter than his proposed 'reasonable expectation' test. Moreover, the 'highly offensive' test goes 'more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which publication was a matter of proper public concern. This could be a recipe for confusion.'[76]

Lord Hope, in formulating his test of what constitutes 'private information' expresses support for the so-called Gleeson test, and held that the Court of Appeal was in error

[72] Ibid. para. 62. [73] Ibid. para. 15. [74] Ibid. para. 21.
[75] (2001) 185 ALR 1 at 13. [76] [2004] 2 WLR 1232 at para. 22.

> . . . when they were asking themselves whether the disclosure would have offended the reasonable man of ordinary susceptibilities. The mind that they examined was the mind of the reader: para 54. This is wrong. It greatly reduces the level of protection that is afforded to the right of privacy. The mind that has to be examined is that, not of the reader in general, but of the person who is affected by the publicity. *The question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity.*[77]

Baroness Hale also gives short shrift to the Gleeson test, declaring:

> An objective reasonable expectation test is much simpler and clearer than the test sometimes quoted from the judgment of Gleeson CJ in the High Court of Australia in *Australian Broadcasting Corporation* v. *Lenah Game Meats Pty Ltd.*[78]

Like Lord Hope, she acknowledges the importance of judging the privateness of the disclosed information from the point of view of 'the sensibilities of a reasonable person placed in the situation of the subject of the disclosure rather than to its recipient'.[79] The learned judge adds:

> It should be emphasised that the 'reasonable expectation of privacy' is a threshold test which brings the balancing exercise into play. It is not the end of the story. Once the information is identified as 'private' in this way, the court must balance the claimant's interest in keeping the information private against the countervailing interest of the recipient in publishing it. Very often, it can be expected that the countervailing rights of the recipient will prevail.[80]

I like to think that these are echoes of my own views expressed first more than twenty years ago. I urged the courts to define what I preferred to call 'personal information'. My own formulation was as follows:

> 'Personal information' consists of those facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold, or at least to restrict their collection, use or circulation.[81]

Any definition of 'personal information' must therefore include both the *quality* of the information and the *reasonable expectations of the individual*

[77] Ibid. para. 99 (emphasis supplied). [78] Ibid. para. 135.
[79] Ibid. para. 136. [80] Ibid. para. 137.
[81] Wacks, *Personal Information*, above n. 2, p. 26; Wacks, *Privacy and Press Freedom*, above n. 2, p. 23.

concerning its use. The one is, in large part, a function of the other. In other words, the concept of 'personal information' postulated here functions both descriptively and normatively. Since 'personal' relates to social norms, to so describe something implies that it satisfies certain of the conditions specified in the norms, without which the normative implications would have no validity. Thus if a letter is marked 'personal', or if its contents clearly indicate that it is personal, the implication is that it satisfies one or more of the conditions necessary for its being conceived as 'personal'; this is a descriptive account.

To the extent that it is necessary to define the information by reference to some objective criterion (since a subjective test would clearly be unacceptable), it is inevitable that the classification depends on what may legitimately be claimed to be 'personal'. Only information which it is reasonable to wish to withhold is likely, under any test, to be the focus of our concern. An individual who regards information concerning say, his or her car, as personal and therefore seeks to withhold details of the size of its engine will find it difficult to convince anyone that the vehicle's registration document constitutes a disclosure of 'personal information'. An objective test of what is 'personal' will operate to exclude such species of information.

The question of the offensiveness of the publication relates to the *publicity* given to the personal information.[82] But there are other considerations, which I examine below.

Putting the record straight

Superstars and supermodels attract little sympathy when they complain of media intrusion. They cannot, it is generally maintained, have it both ways. They bask in the glory of favourable publicity; they cannot therefore legitimately whinge when a disclosure reveals them in a less than satisfactory light. But this down-to-earth judgment neglects the principal purpose of the legal protection of personal information against its gratuitous disclosure. A law that purports to defend the individual against unwanted publicity fails in that objective when it is founded on this popular, but misconceived, notion.

There is, *a fortiori*, even less sympathy for public figures who lie. Indeed, as I noted earlier, Campbell conceded at trial that because she had lied about her drug addiction, the media had a right to put the record straight:

[82] The New Zealand Court of Appeal in *Hosking* v. *Runting* [2005] 1 NZLR 1 appears to have adopted this approach.

there is a public interest in the press revealing the truth. This proposition was vigorously maintained by all five judges in the House of Lords. But why? Suppose that a celebrity were HIV-positive or suffering from cancer. Can it really be the law that a legitimate desire on their part to deny that they are sufferers of one of these diseases may be annihilated by the media's right to 'put the record straight'? If so, the law's purported protection of privacy or confidence is a rather fragile thing. It is submitted that truth or falsity cannot be allowed to block the reasonable expectations of those who dwell in the glare of public attention.

As discussed above,[83] it is not entirely surprising that the courts should be content to oversee the withering away of the distinction between 'privacy' and 'confidence', since the adoption of the Human Rights Act in 1998. As Phillips LJ put it in *Naomi Campbell*:

> The development of the law of confidentiality since the Human Rights Act came into force has seen information described as 'confidential' not where it has been confided by one person to another, but where it relates to an aspect of an individual's private life which he does not choose to make public. We consider that the unjustifiable publication of such information would better be described as breach of privacy rather than breach of confidence.[84]

Seven: Judicial Preference for Legislation

It has become almost routine for judges, especially in England, to manifest a reluctance to 'make law' in this field, and to express the view that the right to privacy 'has so long been disregarded here that it can be recognised only by the legislature'.[85] The advent of the Human Rights Act 1998 (and, to a lesser extent, the Data Protection Act 1998), along with the expansion of the equitable remedy for breach of confidence, have naturally impeded any judicial creativity that might otherwise have evolved.

[83] See above nn. 34–6 and accompanying text.

[84] *Campbell* v. *MGN Ltd* [2003] QB 633 at para. 70.

[85] *Kaye* v. *Robertson* [1991] FSR 62 at 71 (Legatt LJ). Similar sentiments were expressed by Glidewell LJ at 66, and Bingham LJ at 70. See too *Malone* v. *Metropolitan Police Commissioner* [1979] Ch 344, 372–81 at 372 (Sir Robert Megarry VC): 'It seems to me that where Parliament has abstained from legislating on a point that is plainly suitable for legislation, it is indeed difficult for the court to lay down new rules of common law or equity that will carry out the Crown's treaty obligations, or to discover for the first time that such rules have always existed.' More recently in *Secretary of State for the Home Department* v. *Wainwright* [2002] QB 1334 at para. 94, Buxton LJ declared: 'It is thus for Parliament to remove, if it thinks fit, the barrier to the recognition of a tort of breach of privacy.'

Many will claim, with some justification, that even if our legislative bodies were genuinely representative, the arguments in support of their being in a stronger position than courts to protect and preserve our rights are, at best, weak. Not only are the vicissitudes of government and party politics notoriously susceptible to sectional interest and compromise, to say nothing of corruption, but it is precisely because judges are not 'accountable' in this manner that they are often superior guardians of liberty. Moreover, the judicial temperament, training, experience, and the forensic forum in which rights-based arguments are tested and contested frequently tend to tip the scales toward their adjudicative, rather than legislative, resolution. Indeed, in several contexts it is difficult to see how the latter would operate in practice. Since the rights in question are, *ex hypothesi*, in dispute, what role could elected parliamentarians play?

I share the numerous misgivings about broad, vaguely expressed rights in international declarations and bills of rights; clearly drafted legislation is invariably preferable. Even so, I concede that one's trust in lawmakers is, alas, rarely vindicated. Though sometimes contentious, certain fundamental rights are best kept off-limits to legislators, or, at least, beyond the reach of normal political machinations. Would the civil liberties of black Americans have been recognised sooner without the Supreme Court's historic *Brown* judgment? Is the South African Constitutional Court more likely to protect human rights than its new, democratic parliament? Have the judgments of the European Court of Human Rights not enhanced civil liberties in Britain?

The present argument rests, however, on a different premise. As I have sought to show, not only have the courts generally failed to enunciate a lucid or coherent remedy against gratuitous publicity, but the increasing complexity of the challenge they face in mediating between privacy and free speech renders the subject a perfect candidate for the creation of a statutory tort.

Conclusion

The long journey toward the judicial recognition of a common law tort of privacy is beset with stumbling blocks. The seven I have identified above will continue to impede any development along American lines. The prospect of the House of Lords (or, indeed, any common law court of final appeal) identifying a new tort of public disclosure of private facts is therefore extremely remote. And similar hindrances thwart the judicial creation of an intrusion tort, though the explanation is, of course, slightly

different.[86] The solution, as I have said, plainly lies in clearly drafted legislation that provides a remedy in tort for unwanted publicity. Key elements include an objective standard of liability (the disclosure would need to be 'seriously offensive to a reasonable person of ordinary sensibilities'), and several defences made available (including the plaintiff's consent, public interest, and privilege).[87] We cannot, and should not, wait for the English judges to act. Godot will arrive sooner.

[86] Among the casualties of the so-called war on terror has been individuals' privacy. In the immediate aftermath of the events of 11 September 2001, politicians, especially in the United States, have understandably sought to enhance the powers of the state to detain suspects for interrogation, intercept communications, and monitor the activities of those who might be engaged in terrorism. But here too 'privacy' has unfortunately grown into an ambiguous concept. This has impeded its effective legal protection. In addition, the elastic notion of 'public interest' frequently facilitates the use of electronic surveillance, telephone tapping, and other forms of surreptitious intrusion. Both problems could be resolved by directing the debate away from the competing *rights* of 'privacy' and 'security' towards a more direct, less intangible solution. By placing the control of personal information at the heart of our deliberations about privacy, we may be able to achieve what the orthodox analysis has conspicuously failed to do. This approach postulates a presumptive entitlement accorded to all individuals that their personal information be collected only lawfully or fairly. Further, once obtained, it may not be used for a purpose other than that for which it was originally given. But I digress. Various aspects of this argument may be found in: Raymond Wacks, 'Towards a New Legal and Conceptual Framework for the Protection of Internet Privacy' (1999) 3 *Irish Intellectual Property Review* 1; 'Privacy and Press Freedom: Oil on Troubled Waters' (1999) 4 *Media & Arts Law Review* 259; 'Privacy and Media Intrusion: A New Twist' (1999) 6 *Privacy Law & Policy Reporter* 48; 'Media Intrusion: An Expanded Role for the Privacy Commissioner?' (1999) 29 *Hong Kong Law Journal* 341; 'Pursuing Paparazzi: Privacy and Intrusive Photography' (1998) 1 *Hong Kong Law Journal* 1; 'What has Data Protection to do with Privacy?' (2000) 6 *Privacy Law & Policy Reporter* 143. This approach is not a panacea. Nor should regulatory control *replace* legal remedies. Many of the problems that beset the conventional analysis cannot be so simply wished away. There is, however, a compelling need to rethink the conceptual underpinnings of privacy if we are to arrest its relentless decline in our disturbing new world.

[87] Proposals along these lines (which include the creation of a tort of intrusion) have recently been made by the Law Reform Commission of Hong Kong in its report, *Civil Liability for Invasion of Privacy*, above n. 23.

8

The 'right' of privacy in England and Strasbourg compared

GAVIN PHILLIPSON

Introduction

It is a theme of great durability in English common law: the judiciary will not – or cannot[1] – develop a general tort of privacy, a refusal recently and most emphatically endorsed by the House of Lords in *Wainwright* v. *Home Office*.[2] However, the thesis of this chapter is that the decision of their Lordships in *Campbell* v. *MGN Ltd*[3] effectively gives rise to precisely such a tort, albeit with the proviso that there must be some misuse of 'information' for a cause of action to lie. While wholly failing to resolve the issue of the horizontal effect of Article 8 in terms of dicta at least,[4] their

Part of the research towards this chapter was done by the author during a visit to the Centre for Media and Communications Law, University of Melbourne, as Research Visitor and Senior Fellow, July–August 2004. The author would like to thank Eric Barendt for his very helpful comments on an earlier draft.

1 As the Court of Appeal said, notoriously, in *Kaye* v. *Robertson* [1991] FSR 62.

2 [2004] 2 AC 406.

3 [2004] 2 AC 457. For comment see: David Lindsay, 'Naomi Campbell in the House of Lords: Implications for Australia' (2004) 11(1) *Privacy Law & Policy Reporter* 4 at 4–11; Jonathan Morgan, 'Privacy in the House of Lords – Again' (2004) 120 *Law Quarterly Review* 563 at 563–6.

4 Broadly, Lord Nicholls appeared to plump for what may be termed 'weak indirect horizontal effect' as I have advocated in 'The Human Rights Act, "Horizontal Effect" and the Common Law: a Bang or a Whimper?' (1999) 62 *Modern Law Review* 824: 'the values enshrined in Articles 8 and 10 . . . are as much applicable in disputes between individuals or between an individual and a non-governmental body such as a newspaper as they are in disputes between individuals and a public authority', *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 17; though his Lordship rather surprisingly also declared that it was unnecessary to decide the point, at para. 18; Lord Hoffmann appeared to be against any form of horizontal effect arising from the Human Rights Act 1988, though he rather oddly remarked that he could see 'no logical ground for saying that a person should have less protection against a private individual than he would have against the state for the [unjustified] publication of personal information', at para. 49; Baroness Hale clearly endorsed strong indirect effect (as advocated by Murray Hunt [1998] *Public Law* 423): 'The 1998 Act does not create any new

Lordships made Articles 8 and 10 of the European Convention on Human Rights (ECHR)[5] the centrepiece of the new cause of action they effectively introduced. My argument that a new tort has been introduced in all but name will be based upon two contentions: first, that the second limb of the breach of confidence action – requiring that there must, in addition to being unauthorised use of confidential information be 'circumstances importing an obligation of confidence'[6]– has been decisively and unambiguously removed; second that the first limb – that the information must have 'the quality of confidence'[7]– has been transformed, the notion that the information must be 'confidential' having, essentially, morphed into a requirement that it be 'private' or 'personal' information. The removal of the limb that most distinguished breach of confidence from a pure privacy action, and the shift from confidential to private information, together amount in effect to the creation of a new cause of action. As Lord Nicholls, one of the dissenters in the judgment, put it: 'The essence of the tort is better encapsulated now as misuse of private information.'

However, by a rather extraordinary coincidence, given that the European Court of Human Rights had left it unclear since 1986 whether Article 8 *required* a remedy in national law against non-state intruders into privacy such as the press,[8] the court decided precisely that point in its decision in *Von Hannover* v. *Germany*,[9] handed down only a few months after *Campbell*. But the decision went much further than simply deciding that such a remedy was required: it *simultaneously* and quite dramatically widened the scope of Article 8 in this context: as will be explained below, the decision on its face appears to make Article 8 applicable to any publication of any unauthorised photographs of a person engaged in any activities other than their official duties. In other words, no sooner had the House of Lords dragged the common law up to the standard of protection *thought* to be required by Article 8 than Strasbourg moved the goalposts – and quite some distance too. Moreover, while

cause of action between private persons. But if there is a relevant cause of action applicable, the court as a public authority must act compatibly with both parties' Convention rights', at para. 132; Lord Hope, somewhat ambiguously appeared to agree with her, at para. 86, whilst Lord Carswell did not expressly comment on the matter.

[5] Protecting the rights to privacy and freedom of expression respectively; each right allows for interference where this is prescribed by law and is necessary in a democratic society in order to achieve a legitimate aim, which includes protection of the 'rights of others'. The ECHR opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952).

[6] The traditional formulation from *Coco* v. *A. N. Clark (Engineers) Ltd* [1969] RPC 41 at 47.

[7] Ibid. [8] In *Winer* v. *UK* (1986) 48 IR 154. [9] (2005) 40 EHRR 1.

Campbell and *Von Hannover* are difficult cases to compare in terms of the view they take of what matters are of legitimate concern to the public, and therefore go to the appropriate balance between press freedom and privacy rights, it appears tolerably clear that a fairly sizeable distance has opened up between English law and Strasbourg on this matter too.

The facts of *Campbell* are quite well-known, given that the House of Lords' decision is the third reported judgment in the case, but in brief, Naomi Campbell complained in an action both in breach of confidence and under the Data Protection Act 1998 after the *Mirror* newspaper had published details of her treatment for drug addiction with Narcotics Anonymous, including surreptitiously taken photographs of her leaving the clinic and hugging other clients. Importantly, these photographs made the location of the NA centre that Campbell had been attending clearly identifiable to anyone familiar with the area.[10] In the trial the information in question was divided into five classes as follows:

(1) the fact of Miss Campbell's drug addiction;
(2) the fact that she was receiving treatment;
(3) the fact that she was receiving treatment at Narcotics Anonymous;
(4) the details of the treatment – how long she had been attending meetings, how often she went, how she was treated within the sessions themselves, the extent of her commitment, and the nature of her entrance on the specific occasion; and
(5) the visual portrayal (through photographs) of her leaving a specific meeting with other addicts.[11]

The applicant had conceded that the *Mirror* was entitled to publish the information in categories (1) and (2) – the vital facts that Campbell was a drug addict and was receiving treatment for her addiction;[12] the dispute therefore centred around whether publishing the further details and the photographs (categories (3)–(5)) could attract liability. The Court of Appeal had found[13] that the extra details in these categories were too insignificant to warrant the intervention of the courts.[14] It was this finding that was overturned by the House of Lords on a three to two majority (Lord

[10] As Lord Nicholls found, *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 5.
[11] Ibid. para. 23.
[12] This was because it was accepted that the press was entitled to expose the falsity of Campbell's previous public statements that she did not take drugs and was not a drug addict.
[13] [2003] QB 633. [14] Ibid. 661.

Hope, Lord Carswell and Baroness Hale in the majority; Lord Nicholls and Lord Hoffmann in the minority).

Von Hannover represented the culmination of a long legal fight by Princess Caroline of Monaco to stop pictures of herself and her children, obtained by paparazzi without consent, appearing in various newspapers and magazines across Europe. The pictures themselves, as discussed further below, were relatively anodyne shots of the Princess engaged in various everyday acts: shopping, horse-riding, at a beach club, a restaurant, and so on. The European Court of Human Rights found, unanimously, that the failure of the German courts to provide her with a remedy in relation to these pictures amounted to a breach of Article 8. However, it is its reasoning on both the scope of private life under Article 8 and its disagreement with the German Constitutional Court on the legitimacy of press comment on the Princess's private life that are of most interest. In particular, it will be argued that the decision, contrary to initial impressions, is open to at least two sharply different interpretations in relation to the scope of Article 8.

Campbell and breach of confidence

Breach of confidence is the critical remedy to consider in English law in terms of the latter's compatibility with Article 8 of ECHR;[15] it is the action that is meant to fill the notorious gap in English law deplored by the Court of Appeal in *Kaye* v. *Robertson*[16] and the route towards achievement of compliance through the common law of the court's own duty to act compatibly with the Convention rights under the Human Rights Act.[17] As Lord Woolf now famously observed in *A* v. *B*:

> Under section 6 of the [Human Rights Act], the court, as a public authority, is required not to act 'in a way which is incompatible with a Convention

[15] The remedy under the Data Protection Act 1998 should also not be disregarded, though it is unlikely to prove popular with litigants because of the (effective) bar it contains on obtaining interlocutory injunctions against the press (s. 32(4)); moreover in most cases the outcome will depend upon the balance the court strikes with the public interest in publication, which is likely to be the same under the Act as under the common law: see ss. 32(1) and (2). For comment see Antony White, 'Data Protection and the Media' [2003] *European Human Rights Law Review* (Privacy Special) 25 (volume also published as Jonathan Cooper (ed.), *Privacy* (London: Sweet and Maxwell, 2003)). The actions in trespass and nuisance are capable of providing some protection for privacy but are severely limited by their linkage to interference with property rights.

[16] [1991] FSR 62. [17] Under Human Rights Act 1998, s. 6(1) and (3).

> right.' The court is able to achieve this by absorbing the rights which articles 8 and 10 protect into the long-established action for breach of confidence.[18]

We turn to the second limb of the action first.

'Circumstances importing an obligation of confidence'

I have dealt elsewhere[19] with the gradual disappearance of the requirement either of a pre-existing relationship[20] or an express promise or agreement as to confidentiality between the parties to fulfil this requirement, and even of the need for any recognisable *communication* between the parties; this was achieved through cases in which the defendant, with no prior relationship with the plaintiff, surreptitiously acquired the information in question without the plaintiff's awareness and was yet held to be under an obligation of confidentiality.[21] I have also analysed the post-Human Rights Act, pre-*Campbell*[22] case law on this point, pointing out that while there were dicta suggesting that no traditional factors were needed to impose a duty of confidence,[23] which could arise purely out of a reasonable expectation of privacy being present and at least one first instance decision which had imposed the duty with no traditional factors being present,[24] the courts had clearly not freed themselves from the shackles

[18] [2003] QB 195 at 202. The Court of Appeal in *Campbell* made the lesser finding that they were bound to 'have regard to' both Articles 8 and 10 in deciding such cases: [2003] QB 633 at 658.

[19] Gavin Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726 at 747–8.

[20] *Stephens* v. *Avery* [1988] Ch 449 at 482; the existence of a pre-existing relationship is 'not [now] the determining factor'.

[21] See, e.g., *Francome* v. *Mirror Group Newspapers* [1984] 1 WLR 892 (information obtained through the use of an unlawful telephone tap); *Shelley Films* v. *Rex Features Ltd* [1994] EMLR 134 (injunction granted to prevent the use of a photograph taken surreptitiously on the film set of Frankenstein); *Creation Records Ltd* v. *News Group Newspapers Ltd* [1997] EMLR 444 (injunction granted to prevent publication of a photograph of an album cover design taken surreptitiously on the set).

[22] That is, prior to the decision of the House of Lords in *Campbell*.

[23] Most famously, Lord Woolf's bold statement in *A* v. *B plc* [2003] QB 195 at 207: 'The need for the existence of a confidential relationship should not give rise to problems as to the law . . . A duty of confidence will arise whenever the party subject to the duty is in a situation *where he either knows or ought to know that the other person can reasonably expect his privacy to be protected*.'

[24] *Venables and Thompson* v. *News Group Newspapers* [2001] 1 All ER 908.

of traditional confidentiality values.[25] The law stood in a state of uneasy ambivalence between its desire to protect privacy and the continuing pull of its roots in confidence. While the second limb of the action had seemingly been disposed of by obiter dicta, in practice it appeared to be in rude health. Article 8 was said judicially to have reshaped the action, but in practice its influence on decisions was negligible or non-existent.[26] The maintenance in practice of confidentiality requirements meant that the courts' attempts to fulfil their duty to mould the common law into a remedy in order to fulfil their duty of acting compatibly with Article 8 were proving a failure. In particular, it should be noted that in *Peck* v. *UK*,[27] the Strasbourg court remarked that one reason for finding that the common law of confidentiality could not have afforded a remedy to Peck was its requirement that there be 'circumstances imposing an obligation of confidentiality', which the court found, would have been unlikely to have been fulfilled in the circumstances.[28]

In terms of its efficacy as a privacy remedy against intrusive journalism, particularly surreptitious photography, the crucial point was that the law still needed to dispense with the requirement for there being some express indications of confidentiality in the situation in which the information was acquired.[29] If this were done, so that the obviously private nature of the information itself could impose an obligation not to publicise it, then

[25] This may be seen in particular, in the way in which the brief sexual relationships in *A* v. *B plc* [2003] QB 195 and *Theakston* v. *MGN* [2002] EMLR 22 were found not to give rise to a duty of confidentiality, despite the fact that the information in question was clearly of a very intimate nature, and should therefore, according to authorities such as *Dudgeon* v. *UK* (1981) 4 EHRR 149 at 165, para. 52 and *Lustig Prean* v. *UK* (1999) 29 EHRR 548 have been treated as a particularly important area of private life, especially deserving of strong protection.

[26] In particular, in the 2004 Court of Appeal decision in *D* v. *L* [2004] EMLR 1, which concerned very intimate information, Article 8 *is not even mentioned* in the judgment, let alone the Strasbourg jurisprudence on the importance of sexual life within Article 8. Instead, the reasoning is dominated by very traditional notions of equity, conscience and clean hands.

[27] (2003) 36 EHRR 41. The case is considered below, but in brief it arose from the complaint of Peck that he had no remedy in respect of the passing of footage of himself in a moment of private anguish following a suicide attempt, captured by CCTV cameras, from a local authority to various media outlets. The UK government tried to argue that breach of confidence could have afforded him a remedy and that therefore domestic remedies had not been exhausted.

[28] Ibid. para. 111.

[29] As in *Shelley Films* v. *Rex Features Ltd* [1994] EMLR 134 and *Creation Records Ltd* v. *News Group Newspapers Ltd* [1997] EMLR 444 and in the *Douglas* v. *Hello!* litigation, below n. 32 and accompanying text.

the action would be substantively transformed into a private facts tort, whether the label of 'breach of confidence' continued to be used as a fig-leaf to conceal the shocking creativity of the common law or not. Given, however, that such a 'development' would in effect dispense with what was traditionally the key requirement of the confidence action – the very requirement indeed that distinguished it from a straightforward privacy tort[30] – it is perhaps not surprising that the case law prior to *Campbell* disclosed a certain amount of ambiguity on this issue.

In this area, it is suggested, *Campbell* has made a decisive contribution. The first, and crucial, point to make concerns the ratio of the judgment: a majority of the House of Lords found liability in confidence in respect of the publication of surreptitiously taken photographs of the model outside Narcotics Anonymous, in the street. What, then, were the 'circumstances imposing an obligation of confidentiality'? There was clearly no pre-existing relationship between Campbell and the photographer; no communication between them; no express or implied promise by the photographer of confidentiality – quite the reverse. All these elements were therefore quite clearly disposed of. As Lord Nicholls put it: 'This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship.'[31]

But the ratio of this case goes much further: *unlike* in cases like *Shelley Films*, or, more recently *Douglas* v. *Hello! Ltd*,[32] in which snatched photographs were remedied on confidence grounds, there were no clear indications here that the scene was intended to be confidential, such as warning signs forbidding photography, or other external indications that the scene was confidential, such as the elaborate security precautions to prevent photography taken at the Douglas wedding. In fact, the only thing that could impose the obligation of confidence in relation to the photographs was the obviously private nature of the information itself – the fact that it concerned therapeutic treatment. This then was the first time that an English appellate court had imposed liability for use of personal

[30] Note that the definition of the US privacy tort stipulates only as to the quality of the information itself. The US tort is defined as follows: 'One who gives publicity to a matter concerning the private life of another is subject to liability to the other . . . if the matter publicised is of a kind that (a) would be highly offensive to a reasonable person and (b) is not of legitimate concern to the public', *Restatement (Second) of the Law of Torts* s. 625D.

[31] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at paras. 13–14.

[32] *Douglas* v. *Hello! Ltd* [2001] QB 967; *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996; *Douglas* v. *Hello! Ltd* [2006] QB 125. In that case, stringent security measures, including body searches of the guests and the sealing off of the part of the hotel used for the wedding had been put in place in an attempt to avoid unauthorised photography of the event.

information, in the absence of any circumstances imposing the obligation save for the nature of the information itself. And if it is the private nature of the information that can itself impose the obligation, then the second limb of confidence effectively ceases to exist: there has to be information of a private nature to fulfil the first limb in any event, so the second limb no longer has any independent content. It has disappeared.[33] 'Breach of confidence' simply becomes an action that protects against unauthorised publicity given to private facts.[34]

This is clear, and unarguable, from the ratio of the case itself. But the Lords did not leave this implicit: they made it explicit in the clearest possible statements. Thus Lord Hope deliberately endorsed the expansive dicta of Lord Woolf cited above.[35] Lord Nicholls – one of the minority – said:

> Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential.[36]

It may be noted that this formulation clearly omits the second limb of the confidence action. Lord Hope went further, saying:

> If the information is obviously private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected.[37]

These dicta precisely carry out the transformative step that the passage from *A* v. *B* cited above[38] had opened the way to. It will be recalled that the dicta discussed above allowed for an obligation of confidentiality to be imposed where there was a reasonable expectation of privacy. Lord Hope now makes clear that the sole element required to give rise to that expectation is the fact that 'the information is obviously private'. This

[33] As acknowledged by Morgan, 'Privacy in the House of Lords – Again', above n. 3.

[34] It should be noted that while the photographs were found to attract liability only by the majority, the minority rejected this finding not on the basis that there was no obligation of confidence, but because of their finding that the photographs contained no information worthy of protection: i.e., that the first limb was not satisfied.

[35] See above n. 23.

[36] [2004] 2 AC 457 at para. 14. Baroness Hale also summarises the essential requirement of the new-style action very clearly: 'The position we have reached is that [prima facie liability is made out] when the person publishing the information knows or ought to know that there is a reasonable expectation that the information in question will be kept confidential' at para. 134.

[37] Ibid. para. 96.

[38] See above n. 23.

spells out in clear terms the demise of the second limb. Its removal gives us, in effect, a privacy tort, whatever the language used by the judiciary to describe it. As we shall see, the 2005 Court of Appeal judgment in *Douglas* v. *Hello! Ltd*[39] while emphatically affirming these developments, seems ready to take a further step in respect of terminology.

At this point, however, it is necessary to take a step backwards from our provincial excitement with developments in English law, seen in isolation. This chapter is comparing the right to privacy that Strasbourg has interpreted Article 8 as requiring, with that which English law has tortuously developed from an old equitable action. As noted above, it was *essential* that English law take the step it now appears to have done, in ridding itself of the second limb of the *Coco* formulation. However, this step, although to be welcomed,[40] merely removes a negative – an element in breach of confidence that *prevented* it from becoming a real privacy remedy. What is of the most pressing concern, now this has seemingly been done, is what has happened to the first limb – in other words, what kinds of information are deemed capable and worthy of protection under the new action for breach of confidence.

What kinds of personal information can be protected under the doctrine of confidence?

Traditionally, to be afforded protection, information had to have the necessary 'quality of confidence'. Prior to *Campbell*, there had been no detailed discussion in the cases of what the proper scope of this requirement should be, in order to ensure harmony with Article 8 of ECHR as interpreted at

[39] [2006] QB 125. This is the decision of the Court of Appeal on the appeal from the decision to award damages at final trial made by Lindsay J: [2003] 3 All ER 996 (*Douglas II)*, the Court of Appeal having in 2001 declined to grant an injunction in the case: [2001] QB 967.

[40] Welcome that is, if one takes the view, as I have consistently done, that English judges will neither declare a general, free-standing tort of privacy (confirmed recently in *Wainwright* v. *Home Office* [2004] 2 AC 406) nor interpret their duties under the HRA as requiring them to give direct effect to Article 8 in private law, as H. W. R. Wade and more recently others, such as Jonathan Morgan, have argued, and that therefore development of breach of confidence is the only *realistic* means towards providing protection for privacy. It is not therefore suggested that breach of confidence provides the *ideal* privacy remedy, merely the only practically available one, given the actual views of the senior judiciary on these matters, and preferable to none. References are to H. W. R. Wade's 'Horizons of Horizontality' (2000) 116 *Law Quarterly Review* 217 and Jonathan Morgan's 'Privacy, Confidence, and Horizontal Effect: '"Hello" Trouble' (2003) 62 *Cambridge Law Journal* 444. On this issue generally, see the chapter by Raymond Wacks in this volume.

Strasbourg; a general test had been laid down (considered below), but it was not, rather surprisingly, one taken from the Strasbourg jurisprudence. Instead, in the typical common law style, decided cases had indicated a number of discrete areas of private life that were worthy of protection.[41] The twin problems that remained[42] were the fact that the general test being used was arguably not in harmony with Article 8 and the persistence of a more general tendency, evident especially in the Court of Appeal decision in *Campbell*,[43] to ignore or marginalise Article 8 when making key findings and gravitate instead back to traditional confidentiality concerns.

The decision of the House of Lords in *Campbell* has gone some way to remedy both these matters. The House recognised that the first port of call in determining whether there are facts worthy of protection should be the Article 8 case law and, secondly, that the test of high offensiveness[44] was therefore not to be used as a *threshold* test, which had to be satisfied in *all* cases, but rather only as a tie-breaker, to determine marginal or doubtful cases and to be used to help determine the weight or seriousness of the privacy interest when balancing it against the competing interest in publication. Their Lordships also avoided the mistake of falling back upon orthodox confidence principles in deciding the case.

Firstly, as to the 'high offensiveness' test, it is worth setting out the relevant passage from *Lenah Game Meats* in full:

[41] These included information relating to sexual life and intimate relations (*A* v. *B plc* [2003] QB 195, confirming findings in *Barrymore* v. *News Group Newspapers Ltd* [1997] FSR 600 and *Stephens* v. *Avery* [1988] Ch 449); see also an unreported decision in 2005 of Bell J in which an injunction was granted against further publication of pictures of a couple in an intimate embrace outside a night club, caught on CCTV: see 'Jagger's Girl Wins Ban on CCTV Pictures', *Daily Telegraph* (London), 10 March 2005. Other types of information that have been protected include: details of a person's address (*Mills* v. *News Group Newspapers* [2001] EMLR 41); photographs of the interior of a home (*Beckham* v. *MGN* (unreported, QBD, Eady J, 28 June 2001)) and of a wedding (the *Douglas* decisions); details of domestic household arrangements (*Blair* v. *Associated Newspapers*, case no. HQ0001236, a number of unreported decisions were delivered in 2001) and of plastic surgery (*Archer* v. *Williams* [2003] EMLR 38); photographs of the nude and semi-nude body (*Theakston* v. *MGN* [2002] EMLR 22 and *Holden* v. *Express Newspapers Ltd* (unreported, QBD, Eady J, 7 June 2001)) and of a child's face used without permission in a local authority brochure (*Jacqueline A* v. *The London Borough of Newham* (unreported, QBD, Garland J, WL 1612596, 16 October 2001)). It was also clear from the earlier decision in *X* v. *Y* [1988] 2 All ER 650 that it covered medical data.

[42] Discussed in Phillipson, 'Transforming Breach of Confidence' above n. 19.

[43] *Campbell* v. *MGN Ltd* [2003] QB 633 at 660–1.

[44] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at para. 42. The test was taken by the Australian High Court from the US tort. It was used by the Court of Appeal in *Campbell* v. *MGN Ltd* [2003] QB 633 at 660 and impliedly approved in *A* v. *B Plc* [2003] QB 195 at para. 11(vii).

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private, as may certain kinds of activity which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.[45]

Essentially, the Court of Appeal, applying this test in the *Campbell* case, had asked itself the question, 'would a reasonable person of ordinary sensibilities, on reading that Miss Campbell was a drug addict have found it highly offensive, or even offensive that the details as to her treatment and the photograph of her leaving the meeting were also published?';[46] it answered this question in the negative. In the House of Lords, Lord Hope found this approach to be wrong in law. In a strongly argued passage, his Lordship made two key findings. First, 'the test [of offensiveness] is not needed where the information can easily be identified as private':[47]

> If the information is obviously private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected. So there is normally no need to go on and ask whether it would be highly offensive for it to be published.[48]

This seems to be the correct reading of the passage just cited: where it is obvious that the information is private, the 'useful practical guide' of the offensiveness test will not be necessary. Second, his Lordship found that the information in question in the case was indeed clearly private in nature:

> The private nature of these meetings [at NA] encourages addicts to attend them in the belief that they can do so anonymously. The assurance of privacy is an essential part of the exercise. The therapy is at risk of being damaged if the duty of confidence which the participants owe to each other is breached by making details of the therapy, such as where, when and how often it is being undertaken, public. I would hold that these details are obviously private.[49]

[45] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at para. 42.
[46] *Campbell* v. *MGN Ltd* [2003] QB 633 at para. 55.
[47] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 94.
[48] Ibid. para. 96. [49] Ibid. para. 95.

Ironically, of course, in *Lenah Game Meats* itself, Gleeson CJ had said that information relating to, *inter alia*, 'health' was 'easy to identity as private'.[50] The UK Court of Appeal had thus misused the very test they had taken from Chief Justice Gleeson, not recognising it as having two stages: (a) is the information obviously private (e.g. related to health, sexual activity, finances etc)? (b) if *not* then it may be useful to ask would its publication be highly offensive to a reasonable person? Since the information the court was concerned with was clearly 'related to health' (as it concerned therapeutic treatment for drug addiction) and therefore fell into part (a) of the test, there was no need to go onto the second part of the test. The 'highly offensive' limb should not have been applied. Lord Carswell confirmed this, stating, 'it is not necessary in this case to ask . . . whether disclosure of the information would be highly offensive to a reasonable person of ordinary sensibilities. It is sufficiently established by the nature of the material that it was private information.'[51] Lord Nicholls also expressed strong reservations about the test:

> [The Gleeson] formulation should be used with care, for two reasons. First, the 'highly offensive' phrase is suggestive of a stricter test of private information than a reasonable expectation of privacy. Second, the 'highly offensive' formulation can all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which publication was a matter of proper public concern. This could be a recipe for confusion.[52]

Baroness Hale similarly found: 'An objective reasonable expectation [of privacy] test is much simpler and clearer than the test sometimes quoted from the judgment of Gleeson CJ.'[53]

Lord Hope then went on to clarify that, when applying the offensiveness test, either in marginal cases, or to assess the *degree* of intrusion represented by the publication, two conditions applied. First, it should be asked not whether the *reader* of the material in question would find its publication offensive, as the Court of Appeal had seemingly suggested, but whether the individual to whom the information related – Campbell in this case – would so find it: 'The mind that has to be examined is that, not of the reader in general, but of the person who is affected

[50] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR at para. 41.
[51] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 166.
[52] Ibid. para. 22. [53] Ibid. para. 135.

by the publicity.'[54] Second, his Lordship clarified that the test is a mixed objective-subjective test:

> Where the person is suffering from a condition that is in need of treatment, one has to try, in order to assess whether the disclosure would be objectionable, to put oneself into the shoes of a reasonable person who is in need of that treatment. Otherwise the exercise is divorced from its context.[55]

In other words, the reasonable person is not cloaked with the *characteristics* of the applicant, but *is* placed in the overall situation he or she is in, in order to assess their hypothetical response to publication. Baroness Hale agreed: '[Gleeson CJ] was referring to the sensibilities of a reasonable person placed in the situation of the subject of the disclosure rather than to its recipient.'[56] Such an approach may be referred to as a 'situationally subjective' test and it is worth noting that it was also put forward recently by the New Zealand High Court, in which Nicholson J remarked:

> But [the test is] what a reasonable person of ordinary sensibilities would feel if they were in the same position, that is, in the context of the particular circumstances.[57]

Taking this approach, Baroness Hale powerfully argued that the publication of the disputed extra details would be very likely to damage Campbell's therapy:

> Revealing that she was attending Narcotics Anonymous enabled the paper to print the headline 'Naomi: I am a drug addict', not because she had said so to the paper but because it could assume that she had said this or something like it in a meeting. It also enabled the paper to talk about the meetings and how she was treated there, in a way which made it look as if the information came from someone who had been there with her, even if it simply came from general knowledge of how these meetings work. This all contributed to the sense of betrayal by someone close to her of which she spoke and which destroyed the value of Narcotics Anonymous as a safe haven for her.[58]

Lord Carswell substantially agreed.[59]

[54] Ibid. para. 99. [55] Ibid. paras. 97–8. [56] *Ibid.* para. 136.
[57] *P* v. *D* [2000] 2 NZLR 591 at para. 39.
[58] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 153.
[59] '[Publication of the extra details] intruded into what had some of the characteristics of medical treatment and it tended to deter her from continuing the treatment which was in her interest and also to inhibit other persons attending the course from staying with it, when they might be concerned that their participation might become public knowledge', ibid. para. 165.

A further point of significant interest is the manner in which the issue of the photographs accompanying the intrusive article was handled, a matter that is important in differentiating a privacy-based approach – essentially concerned with issues of intrusion and harm – from one based on confidentiality – one concerned with whether the information revealed by photographs can be said itself to be confidential. It should first of all be noted that their Lordships do not appear to find the fact the photographs were taken in the street to be problematic in terms of imposing liability *given what they portrayed*. This being the case, the *ratio* of the case inescapably provides that activities taking place in the street – a fully public location, may yet be protected, if sufficiently sensitive. This amounts to full acceptance of the 'public domain' implications of the previous Strasbourg decision in *Peck* v. *UK*[60] and means that the new action provides a generous measure of protection for privacy in public places. This aspect of the finding is particularly important in evidencing the abandonment in *Campbell* of tests based upon the *confidentiality* of the information, as opposed to its private character. It would clearly seem inapt to describe events taking place in the street, witnessed by numerous people as 'confidential'. This indeed is precisely the line taken by Morgan in a recent article:[61] his starting point is that confidentiality and privacy 'are radically different qualities, and, in particular, [that] much private information is not confidential'.[62] He cites the very fact that information 'in the public domain' cannot be protected under the law of confidence as evidence for this proposition, including specifically within the category of information that cannot be protected, photographs of an individual in a public space. The fact that such information *was* protected in *Campbell* establishes that the question now being asked is whether the information relates to private life, *not* whether it is confidential.

In terms of the treatment of the photographs specifically, for Lord Nicholls and Lord Hoffmann, once it had been determined that publicising the further details in categories (3) and (4)[63] did not engage the applicant's private life, it followed as a matter of logic that the photographs, which merely conveyed the information in those categories (and did not portray Campbell in some embarrassing or undignified act or situation)[64]

[60] (2003) 36 EHRR 41. For discussion of the implications of *Peck* for English law, see Phillipson, 'Transforming Breach of Confidence', above n. 19, 735–40.

[61] Jonathan Morgan, 'Privacy, Confidence, and Horizontal Effect: "Hello" Trouble' (2003) 62 *Cambridge Law Journal* 444 at 452.

[62] Ibid. [63] Above n. 11 and accompanying text.

[64] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 31 (Lord Nicholls) and para. 76 (Lord Hoffman).

added nothing to the applicant's claim. Lord Nicholls was clear that the greater distress caused by the publication of the photographs was legally irrelevant:

> The complaint regarding the photographs is of precisely the same character as the nature of the complaints regarding the text of the articles: the information conveyed by the photographs was private information. Thus the fact that the photographs were taken surreptitiously adds nothing to the only complaint being made.[65]

The approach, then, is very much a formalistic one: the distress occasioned by the surreptitious photography is real, but, since the issue is purely to do with whether sufficiently sensitive *private facts* were revealed, that distress cannot be slotted into any of the limbs of the cause of action the court must consider. It must therefore be disregarded. In contrast, Lord Hope finds the effect of the photographs upon Campbell to be, not only relevant, but in fact the *crucial factor* that leads him to find against the newspaper.[66] This finding, it transpires, is based upon the likely *impact* of the publication of those photographs:

> Any person in Miss Campbell's position, assuming her to be of ordinary sensibilities but assuming also that she had been photographed surreptitiously outside the place where she been receiving therapy for drug addiction, would have known what they were and would have been distressed on seeing the photographs. She would have seen their publication, in conjunction with the article which revealed what she had been doing when she was photographed and other details about her engagement in the therapy, as a gross interference with her right to respect for her private life.

Baroness Hale similarly finds that the publication of the photographs 'added to the potential harm, by making Campbell think that she was being followed or betrayed, and deterring her from going back to the same place again'.[67] Lord Hope and Baroness Hale thus find a way in which the distressing impact of the photographs on someone in Campbell's situation *can* enter the legal equation: they do not go to the question of whether the facts are private or not, as the test from *Lenah* suggests; rather they go to the issue of how offensive and damaging the *publicity* given to those facts is, as a means of evaluating the overall *weight* of the privacy claim. Since the question of whether the publicity given to the relevant facts

[65] Ibid. para. 30 (emphasis added). [66] Ibid. para. 121. [67] Ibid. para. 155.

is offensive self-evidently includes the *manner* in which those facts are publicised (in this case by the use of surreptitiously taken photographs), then those photographs, by this route, become legally relevant once more. This more imaginative approach allows for the overall impact of the entire publication under consideration – including the means used to acquire its contents – to be assessed. In this way, the 'offensiveness' test provides a means to a more holistic assessment of the impact on the applicant's private life and is thus to be welcomed. But this is quite a different matter from using it as a threshold test that must be fulfilled in every case.

Finally, it should be noted that the House of Lords, in dealing with this limb of the action – traditionally, whether the information has the quality of confidence about it – decisively moved the terminology and the underlying concern of the law away from notions of confidentiality towards a concern with privacy. As Lord Nicholls put it, 'Essentially the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy.'[68] Rather than speaking of whether the information is 'confidential', the question now seems to be whether 'the published information engaged Article 8 at all by being within the sphere of the complainant's private or family life'.[69] Article 8 therefore becomes the touchstone for the fulfilment of the first – now the only substantive – limb of the action. Whilst Lord Hope's speech has a heading, '*Was the information confidential?*',[70] his Lordship goes on to state firmly: 'The underlying question in all cases where it is alleged that there has been a breach of the duty of confidence is whether the information that was disclosed was private and not public.'[71] Later in his speech, his Lordship referred to 'the right to privacy, which lies at the heart of the breach of confidence action'.[72] What is taking place here is an explicit reorientation of the underlying normative values of the action. Lord Nicholls declared: 'This tort, however labelled, affords respect for one aspect of an individual's privacy. That is the value underlying this cause of action.'[73] Even more boldly he added:

> the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.[74]

[68] Ibid. para. 21. [69] Ibid. para. 20 (Lord Nicholls). [70] Ibid. para. 88.
[71] Ibid. para. 92. [72] Ibid. para. 105. [73] Ibid. para. 15. [74] Ibid. para. 14.

Lord Hoffmann was even more explicit:

> . . . the new approach takes a different view of the underlying value which the law protects. Instead of the cause of action being based upon the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity – the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.[75]

This is strong (albeit technically indirect)[76] horizontal effect: the dominant normative values are taken from the right to privacy, from Article 8, not from the action for confidence. It amounts to the adoption of the methodology that I have described, under which 'breach of confidence [is] treated simply as an empty shell into which Article 8 principles [are] poured'.[77] How far this process has gone may be seen in Lord Carswell's conclusion, which does not mention breach of confidence even formally:

> I would accordingly hold that the publication of the third, fourth and fifth elements in the article constituted an infringement of the appellant's right to privacy that cannot be justified and that she is entitled to a remedy.[78]

These dicta, then, represent the moment at which 'breach of confidence' becomes a label only: the values traditionally underpinning the action are explicitly and openly replaced with those deriving from the human right to privacy.

The Court of Appeal in its 2005 decision in *Douglas v Hello!*,[79] the only major case so far decided since *Campbell*, was presented, in a sense, with a choice as to how it 'read' or 'presented' the House of Lords' decision. While it is of course a subordinate court, it is not unknown for lower courts to 'read down' or 'expand' judgments of higher courts, diminishing or greatly enlarging their transformative effect. In this respect, the clear effect of *Douglas III* is to emphasise the more transformative aspects of the *Campbell* decision. Thus the radical dicta of their Lordships are highlighted; more conservative dicta or tendencies are not cited. Lord Nicholls' dicta as to the awkwardness of referring to confidentiality

[75] Ibid. para. 51.

[76] Because the applicant must still use an existing cause of action, rather than simply alleging breach of Article 8, without more, as their cause of action – which would be 'direct' horizontal effect, in the jargon.

[77] Phillipson, 'Transforming Breach of Confidence', above n. 19, 731.

[78] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 171.

[79] [2005] HRLR 27 (Court of Appeal judgment on appeal from final trial); hereafter *Douglas III*.

instead of privacy are foregrounded, as are the expansive dicta of Lord Hoffmann that refer to the shift in the values underlying the action from 'the duty of good faith' to 'the protection of human autonomy and dignity'.[80] The court accepts that the basis of the action is now the notion of a 'reasonable expectation of privacy', picking up on the congruence between Lord Hope and Baroness Hale in the majority as to the basic test for the action,[81] and its purpose – the protection of 'the individual's informational autonomy'.[82] Finally, the court gives its own succinct summary of the development of this area of law:

> Megarry J in *Coco* v. *A N Clark* identified two requirements for the creation of a duty of confidence. The first was that the information should be confidential in nature and the second was that it should have been imparted in circumstances importing a duty of confidence. As we have seen, it is now recognised that the second requirement is not necessary if it is plain that the information is confidential, and for the adjective 'confidential' one can substitute the word 'private'.[83]

In the result, the court sums up the sole requirement now needed to make out a prima facie case:

> What the House was agreed upon was that the knowledge, actual or imputed, that information is private will normally impose on anyone publishing that information the duty to justify what, in the absence of justification, will be a wrongful invasion of privacy.[84]

It is now clear beyond doubt, then, that a person acquiring information can come under a legal duty not to publicise it simply by nature of its obviously private character. Remarkably, and in this respect eschewing some of the coyness of the House of Lords in *Campbell*, the Court of Appeal was prepared quite openly to discard even the label of 'breach of confidence'. Thus in a striking phrase, the court remarked:

> We conclude that, in so far as private information is concerned, we are required to adopt, as the vehicle for performing such duty as falls on the courts in relation to Convention rights, the cause of action *formerly described as breach of confidence*.[85]

[80] Ibid. para. 51 of the HL judgment; cited at para. 79 of the CA judgment in *Douglas III* [2006] QB 125.
[81] *Douglas III* [2006] QB 125 at para. 80. [82] Ibid. para. 81.
[83] Ibid. para. 83. [84] Ibid. para. 82. [85] Ibid. para. 53.

The label, it appears, has also now disappeared: the courts have completed the transformation of breach of confidence into what may now be termed 'the tort of misuse of private information'.[86]

The meaning of 'private life' after *Von Hannover* contrasted with *Campbell*

The finding and reasoning in Von Hannover

It was hinted above that the *Von Hannover* decision represents, to say the least, a radical extension of the court's jurisprudence. To bring this point out, it is necessary to recall the facts of the case in a little more detail. The photographs about which Princess Caroline complained in this case showed her engaged in various, mainly everyday activities, including: having dinner in a garden restaurant with a boyfriend; riding on horseback; being out with her children; canoeing; shopping with her boyfriend and son; on a skiing holiday; kissing a boyfriend; leaving her home in Paris; playing tennis, and dressed in a swimsuit at a beach club. The German courts had allowed her to recover only in relation to pictures which captured her in moments in which, while technically in a public space, she had clearly 'sought seclusion' (e.g. by withdrawing to a quiet corner of the garden restaurant with her boyfriend).[87] On final appeal, the Federal Constitutional Court found that the pictures with her children should additionally be entitled to protection, because the right to family protection was also engaged. However, they dismissed her complaint in relation to the remainder of the photographs. This was primarily on the basis that:

> as a figure of contemporary society '*par excellence*', the applicant had to tolerate the publication of photos in which she appeared in a public place even if they were photos of scenes from her daily life and not photos showing

[86] As Lord Nicholls says in *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 14: 'The essence of the tort is better encapsulated now as misuse of private information.' The question whether the action in fact falls to be treated as a tort or an equitable action is beyond the scope of this chapter, though it may be noted that the Court of Appeal took the latter view: *Douglas III* [2006] QB 125 at para. 9.

[87] The Federal Constitutional Court defined a secluded place as 'away from the public eye – where it was objectively clear to everyone that [the couple] wanted to be alone and where, confident of being away from prying eyes, they behaved in a given situation in a manner in which they would not behave in a public place. Unlawful interference with the protection of that privacy could therefore be made out if photos were published that had been taken secretly and/or by catching unawares a person who had retired to such a place', quoted in *Von Hannover* at para. 23.

> her exercising her official functions. The public had a legitimate interest in knowing where the applicant was staying and how she behaved in public.[88]

Thus it is important to note that the European Court was concerned *not* with the pictures of the Princess with her children or those of her dining with her boyfriend in the garden restaurant, but with the less sensitive remainder of the pictures: those showing her shopping, playing tennis, leaving her apartment, and so on. These were *not* then photographs that portrayed her engaged in some 'private act' in the sense in which we have been discussing it so far. The position is clearly markedly different from the situation in *Peck*, in which the applicant was photographed in a public place at a moment of great sensitivity and emotional distress. Moreover, the wording of the judgment in *Peck* had appeared to indicate that private life will only exceptionally be engaged in a public space: 'There is, therefore, a zone of interaction of a person with others, *even in a public context*, which may fall within the scope of "private life".'[89] This suggests that there may need to be exceptional factors present to give rise to a finding that Article 8 applies. In *Peck*, these were clearly the intensely personal and emotional moment captured by the CCTV cameras. In *Von Hannover*, not only was the applicant in a public place, but the activities she was engaged in did not, at first blush, appear to concern private facts at all. Nevertheless, the court expressed no hesitation at all in making its key finding:

> In the present case, there is no doubt that the publication by various German magazines of photos of the applicant in her daily life either on her own or with other people falls within the scope of her private life.[90]

In light of the above considerations, it is rather surprising that the court does not identify *why* the photographs in question relate to private life; they did not, in many cases fall into a 'zone of interaction . . . with others' as many (those picturing her alone) did not concern her relations with anyone. No distinction is drawn by the court between the different photographs in this respect.

The problem perhaps is that the words 'public' and 'private' are being used by the court (without explication or argument) to mean something very much more expansive than their normal meaning in legal discourse. The word 'private' appears to be being used to describe all those aspects of a person's life that do not relate to their official duties. So, for example, a

[88] Ibid. [89] *Peck* v. *UK* (2003) 36 EHRR 41 at para. 57 (emphasis added).
[90] Ibid. para. 53.

civil servant is engaged in her private life all the time, except when carrying out her duties as a civil servant. Buying groceries, is, in this sense, a part of her private life. There is certainly one sense in which we understand this to be the case: a basic distinction between public (in the sense of 'official') and personal or private life. That this is the sense in which the words have been used is indicated by a passage in which the court 'points out' that:

> the photos of the applicant in the various German magazines show her in scenes from her daily life, thus engaged in activities of a purely private nature such as practising sport, out walking, leaving a restaurant or on holiday.[91]

The word 'private' here is clearly being used to mean 'non-official'; the word 'public' to mean, 'part of one's official life or duties'.

The difficulty is that there is another way in which the words are commonly used – perhaps the way that we would expect in this context and in which the other judicial decisions examined so far have used them. In this sense of the word, 'private life' means those aspects of a person's non-official life for which they would generally seek seclusion, intimacy or confidentiality: sexual life, nudity and bodily functions; health, private finance, family life and any activity carried on within the home. Moreover, the word 'public' in discourses about privacy, is usually used not only to mean 'official' (although we do sometimes use it in that way, when talking of 'public life'); it also often means a public *location*: that is, publicly accessible spaces in which the individual can exert no control over who sees her. We would not expect the right to private life to extend to such spaces unless, as the German courts said,[92] a person had sought seclusion for the enjoyment in public of an aspect of private life, for example, sunbathing topless on a secluded beach. Alternatively, there could be a privacy complaint where, although the location was highly public, the activity in question was particularly sensitive – leaving an abortion clinic, perhaps, or, in Campbell's case, a branch of Narcotics Anonymous, or experiencing the aftermath of a suicide attempt, as in *Peck*. But absent some such particularly personal or intimate aspect, normal activities carried on in public – walking, shopping, eating, riding a cycle or horse, are not, in this sense, generally seen as part of 'private life' in the Article 8 sense. Scholars tend to define 'private facts' much more restrictively. W. A. Parent's proposed definition of personal information, for example, is 'information about a person which most individuals in a given time do not want widely known

[91] Ibid. para. 61. [92] See above n. 87.

[or which] though not generally considered personal, a particular person feels acutely sensitive about'.[93] The fact that one has been shopping, or riding a horse would not appear to fall into either category, although in relation to Princess Caroline, there is an argument that it falls into the second category – a restrictive reading of the Strasbourg court's judgment that will be considered in a moment. This was indeed precisely the reason why the applicants in the recent decision in *Hosking* v. *Runting*,[94] although they succeeded in persuading the New Zealand Court of Appeal that there was a tort of invasion of privacy, lost their case on the facts. The complaint was of the publication of pictures taken without consent of a celebrity couple's young children in a busy street. The action failed both because of the very public location in which the pictures were taken, and because they revealed nothing sensitive or intimate about the couple or the children themselves. While aspects of the decision are open to criticism, its whole approach is that only particular aspects of a person's life will be considered to fall within the sphere of 'private life' in human rights terms. As Gleeson CJ put it in the dicta discussed above from *Lenah Game Meats*: '*Certain kinds* of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private, as may *certain kinds* of activity.'[95]

To give an example, it could be argued along these lines that a photograph simply showing a person coming out of a supermarket with a trolley of shopping does not engage private life: it merely reveals the anodyne fact that the person in question has shopped for groceries – scarcely an intimate or sensitive matter. However, if, for example, a reporter surreptitiously followed a woman shopping in a chemist and managed to record that she had purchased a particular prescription drug, or contraceptives, or a pregnancy testing kit, then publication of such information *would* engage private life – because the items purchased all relate to highly personal and intimate matters: health, sexual life and reproduction. Moreover, the customer buying them would not expect the details of her purchases to be seen except by a very few others in the shop. Such distinctions, it may be suggested, are fine but vital ones, if the meaning of 'private life' in public is to be kept within manageable limits. Remarkably, the Strasbourg court here draws no such distinctions.

[93] W. A. Parent, 'A New Definition of Privacy for the Law' (1983) 2 *Law and Philosophy* 305 at 306–7.
[94] [2005] 1 NZLR 1.
[95] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at para. 42.

Von Hannover *vs* Campbell *on the scope of private life: can the decisions be reconciled?*

In order to answer this question, it is necessary to recall for a moment what the new-style 'tort of misuse of private information' or 'new-style breach of confidence' now requires. As discussed above, the sole element that the applicant must now show in English law is that he or she had a 'reasonable expectation of privacy' in the information disclosed by the respondent. Once that threshold has been crossed, the courts will then turn to balancing the privacy interest against the expression interest of the respondent.[96] We know further that where the information concerned is 'obviously private', such a reasonable expectation will exist. If it is not, then the issue of whether its disclosure would be highly offensive to the applicant may be examined, presumably along with any other relevant factors, such as the location in which the applicant was when any photographs were taken, the means used to obtain them and the likely effects upon the applicant of publication. The speeches of the majority in *Campbell* have been criticised for leaving the new test so unclear. As Moreham comments:

> Unfortunately, however, Lord Hope gave no indication of how a court might go about determining whether information is 'obviously private': he simply said that the fact that group therapy is widely recognised as effective treatment for drug addiction and that anonymity is an important part of that process meant that the requirement was satisfied in that instance. This seems problematic: one need only refer to the fact that two members of the House of Lords and a unanimous Court of Appeal held that what was 'obviously private' to Lord Hope was not private at all, to highlight the uncertainty such a requirement could create.[97]

This, however, is incorrect. The view of the Court of Appeal and the dissenters in the Lords was essentially that once it had been conceded that the information in the first two categories could be publicised, the remaining details were not significant enough to deserve protection. But *all* the judges involved in the case, and indeed, the *Mirror* itself, agreed that all of it was information that Campbell would have been entitled to keep private had she not told public lies about it.[98] In other words,

[96] A matter considered below.

[97] N. A. Moreham, 'Recognising Privacy in England and New Zealand' (2004) 63 *Cambridge Law Journal* 555 at 556.

[98] See Lord Nicholls, *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 24: 'It was common ground between the parties that in the ordinary course the information in all five categories

all the judges in this case *did* recognise these details as 'obviously private'. Moreover, Moreham's broader point does not take account of the extensive citation of Article 8 case law: for example, the finding in *Z* v. *Finland* that, 'the protection of . . . medical data is of *fundamental importance* to a person's enjoyment of his or her right to respect for private . . . life'[99] was quite evidently a major reason for the finding that the information was obviously private. Moreover, Lord Nicholls, as noted above, spoke of determining whether the information fell within the remit of Article 8.[100] In other words, the test propounded – of a reasonable expectation of privacy, of whether the information is obviously private – is to be structured by reference to the Article 8 case law. Of course in this particular case, their Lordships took account of a variety of other factors – the duty of confidentiality lying upon those attending at NA, the harm that could be caused by its breach, and the fact that the case concerned therapeutic treatment, amongst others. But it is quite evident that their Lordships took the view that only certain classes of information would qualify as being 'obviously private' – as the citation of *Lenah Game Meats* itself indicates.

What then is the essential point of difference here between Strasbourg and English law? On its face, it is this: bearing in mind the anodyne nature of the photographs at issue in *Von Hannover*, and the very broad scope to 'private life' given in that case, the Strasbourg decision appears to take the view that any publication of an unauthorised photograph specifically taken of a particular person[101] engaged in an everyday activity outside their official duties will involve a *prima facie* violation of Article 8, a reading of the case that I shall refer to as 'the absolutist view'. In contrast, under English law, the applicant must identify information that relates to a specific aspect of private life, as more narrowly understood, such as health, sexuality and the like. The difference is apparent at its starkest in the speech of Baroness Hale:

> We have not so far held that the mere fact of covert photography is sufficient to make the information contained in the photograph confidential. *The activity photographed must be private.* If this had been, and had been

would attract the protection of article 8'. The Court of Appeal had made exactly the same finding: *Campbell* v. *MGN Ltd* [2003] QB 633 at para. 38.

[99] (1998) 25 EHRR 371 at para. 95 (emphasis added).

[100] Above n. 69 and accompanying text.

[101] The words 'specifically taken of a particular person' are used because this judgment would presumably not apply to photographs of normal street scenes in which individuals happen to be caught.

> presented as, a picture of Naomi Campbell going about her business in a public street, there could have been no complaint . . . If . . . she pops out to the shops for a bottle of milk . . . there is nothing essentially private about that information nor can it be expected to damage her private life.[102]

Lord Hoffmann appeared to agree:

> In the present case, the pictures were taken without Ms Campbell's consent. That in my opinion is not enough to amount to a wrongful invasion of privacy. The famous and even the not so famous who go out in public must accept that they may be photographed without their consent, just as they may be observed by others without their consent.[103]

Baroness Hale's comment that publications showing such pictures 'may not be a high order of freedom of speech but there is nothing to justify interfering with it'[104] is particularly significant. It can only be interpreted as meaning that in such a case, Article 8 would simply not be engaged, precisely the converse of the finding in *Von Hannover*.

Can the two decisions be reconciled? Of course, it should be recalled that while under the Human Rights Act the UK courts are bound to act compatibly with 'the Convention rights' themselves,[105] they are not bound by the Strasbourg jurisprudence; it is something they must only take into account.[106] But assuming that the English courts will not wish flatly to disobey or disregard *Von Hannover*, it may be assumed that they will seek to reconcile the two decisions.[107] Interestingly, the Court of Appeal in *Douglas III*, the only major decision taken since the two judgments came out, did not even advert to the obvious differences between the two, let alone suggest how they could be resolved. To do so was not necessary in the case in hand, but at some point the issue will arise. When it does, there will be two obvious courses of action. One will be to interpret *Campbell* as simply holding that private facts are those falling within the scope of Article 8, as defined by the Strasbourg jurisprudence, now including *Von Hannover*. This, however would have the effect of broadening enormously

[102] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 154 (emphasis added).
[103] *Ibid.* para. 73.
[104] *Ibid.* para. 154.
[105] Section 6(1). In fact of course the decision in *Campbell* does not make it clear whether this is an absolute duty in the sphere of private common law: see above n. 4.
[106] Section 2(1).
[107] Lord Slynn has said that, 'In the absence of some special circumstances . . . the court should follow any clear and constant jurisprudence of the European Court of Human Rights': *R* v. *Secretary of State for the Environment, Transport and the Regions, ex p. Holding & Barnes plc* [2003] 2 AC 295 at para. 26; a finding since affirmed in *R* v. *Secretary of State for the Home Department, ex p. Anderson* [2003] 1 AC 837 at para. 18 (Lord Bingham).

the reach of the common law; given the historic caution of the English judges in relation to privacy, such a course seems most unlikely. However, it should be noted that it is possible to find in *Campbell* some evidence that English law may be prepared to accept such an extension.

First of all, there is the almost teasing hint in Baroness Hale's speech that the common law may not have exhausted its evolution in this respect: 'We have not *so far* held that the mere fact of covert photography is sufficient to make the information contained in the photograph confidential.'[108] Second, some little noticed dicta of Lord Hoffmann add an important caveat to the notion that the act photographed 'must be private'. His Lordship comments:

> Likewise, the publication of a photograph taken by intrusion into a private place (for example, by a long distance lens) may in itself be such an infringement, even if there is nothing embarrassing about the picture itself: *Hellewell* v. *Chief Constable of Derbyshire* [1995] 1 WLR 804, 807.[109]

This in fact is either a simple mistake, or a judicial sleight of hand: for, while purporting simply to cite a principle established in *Hellewell*, these dicta actually *extend* that principle.[110] For in that case, Laws J referred to a photograph being taken of someone 'engaged in some private act'. As Lord Hoffmann puts it, the requirement of some 'private act' – precisely what Baroness Hale insisted upon in relation to photography in a public place – is seemingly dropped. Thus anyone photographed *in a private place*, regardless of the nature of what they are doing, can claim a prima facie infringement of private life. Lord Hoffmann appears here to be suggesting a two-tier standard: in a public place, the applicant must show that the nature of the act was private (embarrassing or humiliating according to Lord Hoffmann specifically); but if photographed in a private place, this is not necessary. In other words, privacy may be locational *or* action-based.

Finally, it should be noticed that Lord Hope was much more receptive, to put it at its lowest, to the position later taken by Strasbourg in *Von Hannover*:

> The taking of photographs in a public street must . . . be taken to be one of the ordinary incidents of living in a free community. The real issue is whether publicising the content of the photographs would be offensive . . . A

[108] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 154 (emphasis added).
[109] Ibid. para. 75.
[110] In fact of course *Hellewell* established no such principle: it merely contained obiter comments to this effect.

> person who just happens to be in the street when the photograph was taken and appears in it only incidentally cannot as a general rule object to the publication of the photograph, for the reasons given by L'Heureux-Dubé and Bastarache JJ in *Aubry* v. *Editions Vice-Versa Inc* [1998] 1 SCR 591, para 59. But the situation is different if the public nature of the place where a photograph is taken was simply used as background for one or more persons who constitute the true subject of the photograph. The question then arises, balancing the rights at issue, where the public's right to information can justify dissemination of a photograph taken without authorisation: *Aubry*, para 61. The European Court has recognised that a person who walks down a public street will inevitably be visible to any member of the public who is also present and, in the same way, to a security guard viewing the scene through closed circuit television: *PG and JH* v. *United Kingdom*, para 57. But, as the court pointed out in the same paragraph, private life considerations may arise once any systematic or permanent record comes into existence of such material from the public domain.[111]

Here, in his apparent acceptance of the *Aubry* position that publication of a photograph taken without consent requires justification, and in entering no qualification that the photograph taken without authorisation must depict a private act of some sort, his Lordship appears to endorse the view that publishing deliberately taken photographs of an individual without consent *does* prima facie engage the right to private life: thus the interest in private life will have to be balanced against 'the public's right to information'. But in this respect, Lord Hope was not supported by his brethren. As the Court of Appeal in *Douglas III* remarked, 'Baroness Hale was not prepared to go this far.'[112] It is apparent, therefore, that while the thrust of the speeches in *Campbell* are incompatible with the absolutist view of *Von Hannover*, there are also harbingers of further movement of the common law in the direction of the latter.

However, given that a wide gulf between the two decisions nevertheless still exists, the other course of action would be to 'read down' the decision in *Von Hannover* to bring it closer to the approach taken in *Campbell*. While the judgments of the Strasbourg court cannot strictly be broken down into 'ratio' and 'obiter dicta', it may be observed that the inferences to be drawn from the finding of a breach in the case and the reasoning the court gives to support that finding are very different. The holding of the case, *given the facts*, is that the systematic and persistent pursuit and photographing of a person going about their everyday life and the publication of those photographs in mass circulation newspapers can give

[111] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 122.
[112] [2005] HRLR 27 at para. 90.

rise to a breach of Article 8. This is not, perhaps, a particularly radical proposition, given the degree of harassment present in the particular case, and the feeling the applicant had of being under constant, albeit unofficial surveillance. As the court put it, under the view taken of Princess Caroline's case by the German courts, the Princess simply 'has to accept that she might be photographed at almost any time, systematically, and that the photos are then very widely disseminated'. The court indeed makes clear that it had this factor very much in mind in coming to the decision it did:

> [The Princess] alleged that as soon as she left her house she was constantly hounded by paparazzi who followed her every daily movement, be it crossing the road, fetching her children from school, doing her shopping, out walking, practising sport or going on holiday.[113]

Indeed the court makes the influence of this factor on its judgment explicit:

> The context in which these photos were taken – without the applicant's knowledge or consent – and the harassment endured by many public figures in their daily lives cannot be fully disregarded.[114]

And again:

> Furthermore, photos appearing in the tabloid press are often taken in a climate of continual harassment w*hich induces in the person concerned a very strong sense of intrusion into their private life* or even of persecution.[115]

The italicised words are of particular significance: they suggest that it is not any one particular photograph, or what it reveals, that induces the sense of intrusion into private life, but, as the court puts it, 'a climate of continual harassment'. This suggests that what we actually have here is a judgment that combines two elements in coming to a finding that Article 8 is engaged: (a) the fact that the pictures relate to the Princess's everyday life, not her official functions, and (b) the constant intrusion that the persistent photographing represents. This more restrictive reading would dovetail nicely with the second part of the definition of private facts proposed by Parent: 'information about a person which . . . though not generally considered personal, a particular person feels acutely sensitive about'.[116] The photographs, in other words, fall within Article 8 because, while not revealing anything generally considered personal, they induce an acute feeling of intrusion because of the persistent campaign of low-level intrusion of which they are a part. Looked at this way, the judgment

[113] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 44.
[114] Ibid. para. 68.
[115] Ibid. para. 59 (emphasis added).
[116] Parent, 'A New Definition of Privacy', above n. 93, 307.

in *Von Hannover* does not, necessarily, imply that *any* photograph taken without consent of a person in their private capacity will engage Article 8; rather the question will be either whether the photograph taken of the person reveals or exposes some intimate aspect of their life (as in *Campbell* or *Peck*) *or* whether the cumulative impact of the persistent taking and publishing of such photographs is such as to give rise to a level of intrusion sufficient to breach Article 8.

It is conceded immediately that this is only one reading of the judgment: it is quite evident that the court nowhere states that it is the cumulative effect of the photography that in this case was the *decisive* factor. Nevertheless, it would be a perfectly defensible course of action for the English courts to interpret *Von Hannover* simply as a finding that the systematic pursuit and photographing of a person as they go about their daily life can, in sufficiently serious circumstances, amount to a breach of Article 8. Such a finding could be accommodated within the new law: while the information in the particular photograph might not be 'obviously private', the publication of the photograph could satisfy the alternative test of being 'highly offensive to a reasonable person of ordinary sensibilities'.[117] Thus, if a case were brought in the English courts that concerned a one-off photograph of, for example, a celebrity jogging in the park, the lack of persistent intrusion would clearly be a distinguishing factor that could lead the court to find that the *Von Hannover* principle was not engaged on the facts and that the information was neither obviously private, nor was its publication highly offensive. Given that the more 'absolutist' reading of *Von Hannover* would have the effect of requiring all Council of Europe states to move to something like the French model of privacy, whereby any unauthorised photography of an individual engaged in non-official activities is a breach of their personality rights, it is suggested that the more nuanced reading suggested here is the more realistic one. This is especially the case given that the absolutist reading effectively removes any margin of appreciation for individual states in a highly controversial area, and one in which markedly different standards apply within Europe.

Privacy and press freedom: the difficult balancing act required[118]

The question of how a right to privacy can be balanced against press freedom is possibly the most difficult problem raised by any privacy law

[117] See above text accompanying nn. 48 and 51.

[118] See Eric Barendt's chapter in this volume for a discussion of the wider theoretical and legal questions surrounding this issue. The discussion here is confined to a specific comparison of the approach of recent Strasbourg and English decisions.

and crucial to its success. Once again, the picture here is of significant movement by English courts towards a proper appreciation of the requirements of Strasbourg principle; indeed, the decision in *Campbell* in this respect is arguably just as significant as its refashioning of breach of confidence as a vehicle for Article 8 rights. However, closer examination of this issue reveals, once again, a significant area of tension remaining between the two legal systems.

The satisfactory resolution of the potential conflict between Articles 8 and 10 must, it is suggested, be found at two levels. First there is the issue of the *structure* of the reasoning process by which the balancing act between the two rights should be undertaken. Second, there is the issue of substance: what principles should the court use to weigh the two rights against each other when carrying out this process?

How should the balancing act be carried out: methodology

The author has analysed elsewhere the serious flaws in the approach of English courts in most of the cases prior to *Campbell* in this respect.[119] In summary, in the mistaken view that Article 10 had some kind of primacy in the Convention scheme,[120] the courts sometimes expressly,[121] sometimes when paying lip-service to the notional equality of the two rights,[122] had treated Article 8 essentially as a mere exception to Article 10. This was, of course, wrong in principle: to treat privacy rights under Article 8 in the same way as the societal interests enumerated in Article 10(2), which are to be narrowly construed,[123] simply collapses the basic

[119] See Phillipson, 'Transforming Breach of Confidence', above n. 19, 748–58. The point has been stressed by other commentators: see Heather Rogers and Hugh Tomlinson, 'Privacy and Expression: Convention Rights and Interim Injunctions' [2003] *European Human Rights Law Review* (Privacy Special) 37 esp. at 48–53; and Basil S. Markesinis, Colm O'Cinneide, Joerg Fedtke and Myriam Hunter-Henin, 'Concerns and Ideas about the Developing English Law of Privacy (and how Knowledge of Foreign Law Might Be of Help)' (2004) 52 *American Journal of Comparative Law* 133 at 153–7; see also M. A. Sanderson's valuable commentary on the *Von Hannover* decision: 'Is *Von Hannover* v. *Germany* a Step Backward for the Substantive Analysis of Speech and Privacy Interests?' (2004) 6 *European Human Rights Law Review* 631 at 642–4.

[120] A view resulting from the misapplication of dicta from the *Sunday Times* case to the effect that where other interests potentially threaten free speech, the issue is not 'a choice between two conflicting principles but . . . a principle of freedom of expression that is subject to a number of exceptions which must be narrowly interpreted': *Sunday Times* v. *UK* (1979) 2 EHRR 245 at para. 65.

[121] *Venables and Thompson* v. *News Group Newspapers* [2001] 1 All ER 908 at 931; *Theakston* v. *MGN* [2002] EMLR 22 at para. 34; *Mills* v. *MGN* [2001] EMLR 41 at [15].

[122] *A* v. *B plc* [2003] QB 195 at paras. 11(iv) and (vii) and 44–8.

[123] *Sunday Times* v. *UK* (1979) 2 EHRR 245 at para. 65.

scheme of the Convention, which, as a human rights treaty, is axiomatically to afford human rights a special status over other interests. But it also had two further effects. First, since the question judicially asked was whether there existed sufficient grounds to justify interference with freedom of expression, the court at no point considered how far that right was really at stake.[124] One of the essential requirements for satisfactory judicial resolution of the conflict between privacy and speech in a given case is that the value of the speech claim, in Article 10 terms, is carefully considered. If this is not done, the courts will have weights for one side of the scales only. In other words, if judges *assess* the weight of the privacy claim, but simply *assume* that of the speech argument, their approach will suffer from a structural imbalance that will preclude a fair resolution of the competing interests at stake. Finally, since the courts in these cases were concerned only with whether the interference with press freedom was justified, they missed the point that stories which both revealed a private fact (e.g. of an affair, or sexual encounter)[125] *and* contained intimate details of it, should be scrutinised through a proportionality lens, in order to determine whether the extra intrusion into private life represented by the detail could be justified by reference to the 'speech value' which those details added.[126]

I have advocated the reversal of all of these mistaken tendencies, and the adoption instead of what may be termed a 'dual exercise in proportionality'[127] or 'parallel analysis', as it has been dubbed;[128] under such an approach, rather than assigning one right a prior position as a mere exception to the other, the courts would have to consider the matter from the point of view of each Convention right in turn. Such an approach requires courts to assess the weight, in Convention terms, of *both* rights[129] and ask not only whether the restriction that the applicant sought to lay on the press is greater than necessary to protect his or her legitimate privacy interests, but also, conversely, whether the story goes further, in terms of intrusive detail, than is necessary to fulfil the media's legitimate function.

[124] This was characteristic of all the major cases prior to *Campbell* (HL): see Phillipson, 'Transforming Breach of Confidence', above n. 19, 756–8.

[125] As in *A* v. *B plc* [2003] QB 195 and *Theakston* v. *MGN* [2002] EMLR 22 respectively.

[126] See Phillipson, 'Transforming Breach of Confidence', above n. 19, 753.

[127] Gavin Phillipson and Helen Fenwick, 'Breach of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 *Modern Law Review* 660 at 687.

[128] Rogers and Tomlinson, 'Privacy and Expression' above n. 119, 50–2.

[129] Markesinis et al, 'Concerns and Ideas', above n. 119, lay particular emphasis upon this aspect of the process, pointing out its success in other jurisdictions, especially German: at 155–7.

The claims of both parties are thus subject to a searching, but balanced examination.

This approach has now been decisively endorsed by the House of Lords, both in *Campbell* and in their recent decision on the appeal from *Re S*.[130] Firstly, all of their Lordships – including Lord Nicholls and Lord Hoffmann – rejected the notion of Article 10 having any presumptive priority. As Lord Nicholls put it:

> The case involves the familiar competition between freedom of expression and respect for an individual's privacy. Both are vitally important rights. Neither has precedence over the other . . .[131]

Lord Hoffmann was more emphatic:

> There is in my view no question of automatic priority [of speech over privacy]. Nor is there a presumption in favour of one rather than the other. The question is rather the extent to which it is necessary to qualify the one right in order to protect the underlying value which is protected by the other. And the extent of the qualification must be proportionate to the need: see Sedley LJ in *Douglas* v. *Hello! Ltd* . . .[132]

Lord Hope took the same view:

> Any restriction of the right to freedom of expression must be subjected to very close scrutiny. But so too must any restriction of the right to respect for private life. Neither article 8 nor article 10 has any pre-eminence over the other in the conduct of this exercise.[133]

Baroness Hale agreed,[134] endorsing her own approach in the Court of Appeal decision in *Re S*. In the subsequent House of Lords decision in that case, Lord Steyn, giving the unanimous opinion of the House, helpfully distilled the approach we have been discussing into four key principles which he said, 'clearly emerge[d] from the speeches' given in *Campbell*:

> First, neither article has as such precedence over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justifications for interfering with or restricting each right must be taken into account. Finally, the proportionality test must be applied to each.[135]

[130] [2005] 1 AC 593. [131] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 12.
[132] Ibid. para. 55. [133] Ibid. para. 113. [134] Ibid. paras. 111 and 138.
[135] *Re S* [2005] 1 AC 593 at para. 17.

As Baroness Hale explained in *Campbell*:

> [The correct balancing approach] involves looking first at the comparative importance of the actual rights being claimed in the individual case; then at the justifications for interfering with or restricting each of those rights; and applying the proportionality test to each.[136]

There is no doubt that this assessment of the importance of each right *in the particular context under examination* is the correct approach in terms of Convention principle: in *Peck*, for example, the court undertook a careful assessment of whether the public interest claimed by the Council – that of publicising the effectiveness of CCTV and thus deterring crime – justified the intrusion into the applicant's private life. It found that it did not, principally because showing images that revealed the applicant's identity could not be seen to be a *necessary* part of furthering that admittedly 'strong' public interest engaged.[137] In *Von Hannover*, the court endorsed the necessity of examining the weight of the competing speech claim – something that, as seen, the English courts had wholly failed to do in the past – in the clearest way:

> The decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the [contested publication] make[s] to a debate of general interest.[138]

The point is the simple one that the weight of any claim under Article 10 should be assessed by reference to the contribution that the publication in question makes to a debate of serious public concern and that where it makes no such contribution, it may readily be overridden by countervailing Convention rights, in this case, Article 8. This point had been resoundingly missed in a number of English decisions prior to *Campbell*. In particular, a notable tendency had been to treat the public interest in a story as wholly separate from the issue of the application of Article 10, taking the view that the latter is fully engaged even where the former is wholly absent[139] and to view all kinds of media expression as monolithic, of unvarying weight.

[136] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 141.
[137] *Peck* v. *UK* (2003) 36 EHRR 41 at para. 79.
[138] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 76.
[139] In *A* v. *B plc*, Woolf CJ said: 'Any interference with the press has to be justified because it inevitably has some effect on the ability of the press to perform its role in society. This is the position *irrespective of whether a particular publication is desirable in the public interest*', [2003] QB 195 at 205 (emphasis added). In *Theakston*, the judge said: 'I can see

On this key point also, the House of Lords in *Campbell* practised what it preached. For the first time in an English appellate privacy judgment we see an attempt to scrutinise not just the value of the *privacy* claim, but the *speech* claim as well. Thus Lord Hope remarked of the latter:

> Clayton and Tomlinson, *The Law of Human Rights* (2000), para 15.162, point out that the court has distinguished three kinds of expression: political expression, artistic expression and commercial expression, and that it consistently attaches great importance to political expression and applies rather less rigorous principles to expression which is artistic and commercial. According to the court's well-established case law, freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and the self-fulfilment of each individual: *Tammer* v. *Estonia* (2001) 37 EHRR 857, para 59. But there were no political or democratic values at stake here, nor has any pressing social need been identified.[140]

As Lord Nicholls acknowledged, 'The need to be free to disseminate information regarding Miss Campbell's drug addiction is of a lower order than the need for freedom to disseminate information on some other subjects such as political information.'[141] Baroness Hale also held that 'there are undoubtedly different types of speech' and that some of those 'are more deserving of protection in a democratic society than others', going on to recite the categories mentioned by Lord Hope:

> This includes revealing information about public figures, especially those in elective office, which would otherwise be private but is relevant to their participation in public life. Intellectual and educational speech and expression are also important in a democracy, not least because they enable the development of individuals' potential to play a full part in society and in our democratic life. Artistic speech and expression is important for similar reasons, in fostering both individual originality and creativity and the free-thinking and dynamic society we so much value.[142]

Applying this approach to *Campbell*'s case, her Ladyship found that:

no public interest in the publication of the details of the [sexual] activity': *Theakston* v. *MGN* [2002] EMLR 22 at para. 75; he nevertheless found that: 'the freedom of expression of the *Sunday People* and of the prostitute [in relation to those details] would be given greater weight than the extra degree of intrusion into the claimant's privacy': at para. 76.

[140] *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 117. [141] Ibid. para. 29.

[142] Ibid. para. 148.

> The political and social life of the community, and the intellectual, artistic or personal development of individuals, are not obviously assisted by poring over the intimate details of a fashion model's private life.[143]

Lord Hoffmann similarly emphatically accepted the use of underlying values as a way of balancing the two interests:

> Take the example . . . of the ordinary citizen whose attendance at NA is publicised in his local newspaper. The violation of the citizen's autonomy, dignity and self-esteem is plain and obvious. Do the civil and political values which underlie press freedom make it necessary to deny the citizen the right to protect such personal information? Not at all . . . there is no public interest whatever in publishing to the world the fact that the citizen has a drug dependency. The freedom to make such a statement weighs little in the balance against the privacy of personal information.[144]

These dicta indicate the long-overdue recognition by English courts in privacy cases that Article 10 does not engage a one-size-fits-all weight, opening the way to a principled resolution of clashes between expression interests and Article 8.

Finally, *Campbell* also demonstrates a clear application of the proportionality test to resolving the case. Thus their Lordships accepted that it must further be asked whether the level of intrusive detail contained in the publication in question went further then was necessary in carrying out the press's legitimate function of informing the public. As Lord Hope put it, 'Decisions about the publication of material that is private to the individual raise issues that are not simply about presentation and editing.'[145] Thus he found:

> It is hard to see that there was any compelling need for the public to know the name of the organisation that she was attending for the therapy, or for the other details of it to be set out.[146]

This indeed was the whole basis for the finding in favour of Campbell by the majority: the publication was examined in terms of the five classes described above[147] and the newspaper was, in effect, asked to justify the greater level of intrusion represented by the publication of the details of treatment and the photographs. The question as to whether that extra detail could be justified was put under the microscope: and it was found that there was no justification for it in terms of the public interest. *Both*

[143] Ibid. para. 148–9. [144] Ibid. para. 56. [145] Ibid. para. 113. [146] Ibid. para. 118.
[147] Above n. 11 and accompanying text.

sides therefore were forced to justify the intrusion into the rights of the others that they sought to make: it was found that Campbell could not justify imposing liability for publishing the basic facts because of the legitimate public interest in them – something she had indeed conceded; but equally it was found that the intrusive details – likely in themselves to cause greater damage to Campbell's attempts to rehabilitate herself than merely reporting her drug addiction – could not be justified. *Both* sides therefore had to give some ground; the case turned upon working out a way of ensuring the minimum impairment of each party's rights. A measure of both privacy *and* of free expression was retained, whereas in the Court of Appeal decision in *Campbell*, as well as in *A* v. *B*, *Theakston* and in *D* v. *L*,[148] expression was allowed full rein, with the result that the competing privacy rights were wholly overridden.

In short, the approach in *Campbell* amounted to a sensitive, contextual balancing exercise, resolved through examination of the value of the two claims and based upon the core Convention principle of proportionality. In this decision, English privacy law comes of age as an effective remedy that pays full regard to freedom of expression as a qualified – not an absolute – value.

The crucial question that remains, however, is the breadth that is assigned to the legitimate role of the press in a democracy. There is full agreement between English courts and Strasbourg that:

> The decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the [contested publication] makes to a debate of general interest.[149]

The question that remains, however, is what kinds of information about private lives can properly be regarded as contributing to such a debate? It is here that there is perhaps an important difference of understanding between Strasbourg and the English courts, though its extent, in this case, remains unclear.

What types of reportage contribute to 'a debate of general interest' and thus fall within the legitimate role of the press in a democracy?

In *Von Hannover*, the court was confronted with a clear clash between the desire of Princess Caroline to be free from intrusive publications about her private life and the press interest in being free to report on her. As noted

[148] [2004] EMLR 1. [149] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 76.

above, it was on the basis of the public interest in free reportage on the matter that the German Constitutional court had refused to grant relief in respect of the complained of photographs, finding that, 'The public had a legitimate interest in knowing where the applicant was staying and how she behaved in public.'[150] The Constitutional Court here founded upon an explanation of the role that even the popular press could play in a democratic society:

> Nor can mere entertainment be denied any role in the formation of opinions. That would amount to unilaterally presuming that entertainment merely satisfies a desire for amusement, relaxation, escapism or diversion. Entertainment can also convey images of reality and propose subjects for debate that spark a process of discussion and assimilation relating to philosophies of life, values and behaviour models. In that respect it fulfils important social functions. . . The same is true of information about people. Personalization is an important journalistic means of attracting attention. Very often it is this which first arouses interest in a problem and stimulates a desire for factual information. Similarly, interest in a particular event or situation is usually stimulated by personalised accounts. Additionally, celebrities embody certain moral values and lifestyles. Many people base their choice of lifestyle on their example. They become points of crystallisation for adoption or rejection and act as examples or counter-examples. This is what explains the public interest in the various ups and downs occurring in their lives.[151]

This is a relatively subtle and sophisticated view of the legitimate role of the media in a democracy, which goes well beyond the overt discussion of political matters or of politicians. As one American commentator has put it, '[The] media uses people's names, statements, experiences, and emotions to personalise otherwise impersonal accounts of trends or developments.'[152] Where such speech is not political, it may not lie at the core of Article 10 protected speech. But, to quote Lord Cooke, 'Matters other than those pertaining to government and politics may be just as important in the community.'[153] Such speech, which can 'inform the social, political, moral and philosophical positions of individual citizens',[154] could include revelations relating to matters as diverse as eating

[150] Quoted in ibid. para. 25. [151] Ibid.

[152] David A. Anderson, 'The Failure of American Privacy Law' in Basil S. Markesinis (ed.), *Protecting Privacy* (Oxford: Oxford University Press, 1999), p. 142.

[153] *Reynolds* v. *Times Newspapers* [1999] 4 All ER 609 at 640.

[154] Diane L. Zimmerman, 'Requiem for a Heavyweight: a Farewell to Warren and Brandeis's Privacy Tort' (1983) 68 *Cornell Law Review* 291 at 346.

disorders, abortion, attitudes to sexuality, education and the like; it will often concern not politicians, but celebrities, their relatives and those who for a short time and for a particular reason only are thrust into the public gaze. However, *instead* of acceding to the above argument to the effect that details as to private lives could form part of a discourse with important public significance (what the German courts referred to as 'infotainment'), the Strasbourg court in *Von Hannover* draws a sharp (and perhaps somewhat simplistic) distinction:

> The Court considers that a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of 'watchdog' in a democracy by contributing to 'impart[ing] information and ideas on matters of public interest' . . . it *does not do so* in the latter case.[155]

Note that the court states flatly, 'it does not do so': this is a blanket denial of the place of reportage of private facts within the press's legitimate, watchdog function. Applying this test in the instant case, the court found:

> The situation here does not come within the sphere of any political or public debate because the published photos and accompanying commentaries relate exclusively to details of the applicant's private life.[156]

The court's finding, on its face, is quite striking: publications concerning private life will *for that reason* lack any public interest and thus attract only a low weight under Article 10. What we have here is a form of definitional balancing. The court does not deny that Article 10 is *engaged*: the phrase, 'In these conditions freedom of expression calls for a narrower interpretation', would seem to suggest that perhaps this type of celebrity reportage falls outside the scope of Article 10 altogether, but this would be a radical departure from the court's previous approach to speech, in which even hardcore pornography has been seen as falling within paragraph 1 of Article 10.[157] Rather, the court seems to concede that Article 10 is *engaged*: if it were not, there would be no need for any balancing exercise at all, but as just noted, it refers to 'the decisive factor in balancing the protection of private life against freedom of expression'.[158] However it appears clear that

[155] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 63 (emphasis added).
[156] Ibid. para. 64. [157] *Hoare* v. *UK* (unreported, ECHR, no. 31211/96, 2 July 1997).
[158] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 76.

the type of speech in question will, as a matter of principle, be afforded a very low weight. This is a species of definitional balancing, because it lays down a general rule to be applied to a particular type of speech, and states that in such circumstances, Article 10 is *as a general rule* to be 'narrowly interpreted', a happier construction of which would be, 'afforded a low weight'.

The court goes on to find:

> . . . the publication of the photos and articles in question, of which the sole purpose was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.[159]

Since the photographs and publications 'made no contribution' to a debate of general interest, the interest in press freedom under Article 10 had to give way to the Princess's privacy interests. In Strasbourg's view, it appears, if the complainant in a privacy case performs no official functions and the photographs merely convey details of their private life, the result is a foregone conclusion: the interest in press freedom gives way to the protection of private life. To put it another way, there is generally no (legitimate) public interest in the publication of such photographs.

Such a view, in ruling out almost in advance the possibility of any speech value in the discussion of private facts, amounts to a strikingly restrictive view of the role of the press. And this is not a position which is properly argued for in the judgment. As Sanderson notes, the court throughout its reasoning in fact relies upon an assertion made early on in the judgment that 'public figures' are those that perform official functions. Once it then finds that the Princess performs no such function, she is automatically excluded from the definition of a public figure, and thus reportage on her private life falls outside the scope of contributing to a debate of general interest, which, Sanderson notes, the court simply treats as being synonymous with debate on purely political matters including the performing of official functions.[160] In other words, the court makes one substantive assertion – that public figures should be considered to be only those that perform official functions, and then simply reverts to circularity, in finding that the Princess is not such a figure, and that

[159] Ibid. para. 65.

[160] Sanderson, 'Is *Von Hannover* v. *Germany* a Step Backward', above n. 119, 636–43. Sanderson points out that the court tends to use 'general interest', 'political' and 'official duties' as interchangeable synonyms for 'public'.

therefore information about her cannot contribute to a debate of general interest.[161]

Before leaving this decision, a further, important point should be noted. It is clear that the court does not preordain that *any* reportage of private life will result in Article 8 rights prevailing over Article 10: it states that 'in certain special circumstances, [the public's right to be informed] can even extend to aspects of the private lives of public figures, particularly where politicians are concerned'.[162] The example that the court had in mind[163] was its earlier decision in *Plon (Société)* v. *France*.[164] In this case the court found a violation of Article 10 in the imposition of a permanent injunction against the distribution of a book published immediately after the death of President Mitterand containing details of the 'grand secret' – the fact that throughout nearly all of his Presidency, Mitterand had known (but had concealed from the French public for ten years) the fact that he was suffering from prostate cancer. The case demonstrates that there are circumstances in which the court is prepared to find that reportage of private lives is part of the legitimate function of the press. It must be said, however, that the judgment is an extremely cautious one in terms of defending media freedom: although the political importance of the revelations contained in the book was extremely high, the court nevertheless found that an interim injunction against publication, lasting some nine months was *not* a violation of Article 10. This was despite the fact that the President was dead, and that, as the court commented:

> . . . the book was published in the context of a wide-ranging debate in France on a matter of public interest, in particular the public's right to be informed about any serious illnesses suffered by the head of State, and the question whether a person who knew that he was seriously ill was fit to hold the highest national office. Furthermore, the secrecy which President Mitterrand imposed, according to the book, with regard to his condition and its development, from the moment he became ill and at least until the point at which when the public was informed (more than ten years afterwards), raised the public-interest issue of the transparency of political life.[165]

In other words, in Article 10 terms, the speech was clearly of the 'highest value', since it went to the heart of the political process in France. To

[161] Ibid. pp. 640–1.
[162] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 64.
[163] Ibid. para. 60.
[164] (Unreported, ECHR, no. 58148/00, 18 May 2004).
[165] Ibid. para. 44.

uphold even a temporary injunction against such speech indicates a strong reluctance to allow even the strongest speech claims to override those of private life, a reluctance which is of some concern and indicates how restrictively Article 10 is read by the court when it collides with privacy rights.

A final point on *Von Hannover* relates to the above-noted dicta – 'in certain special circumstances, [the public's right to be informed] can even extend to aspects of the private lives of public figures, *particularly* where politicians are concerned'.[166] This statement is arguably in tension with an important statement of principle from the court's decision in *Thorgeirson* v. *Iceland*[167] to the effect that there is no warrant in its case law for 'distinguishing between political discussion and discussion of other matters of public concern'. The whole tenor of the judgment in *Von Hannover* is against there being a legitimate public concern in issues arising from the private lives of others, with politicians being adduced as the key exception. However, if there is no warrant for distinguishing between political speech and speech on other matters of legitimate public concern, and given that the private lives of non-political actors such as celebrities *can* furnish examples to stimulate debate on matters of serious (although not political) concern, it is evident that a consistent application of the court's jurisprudence should afford a rather broader defence of privacy-invading speech than the court appears to admit here.

Perhaps one reason why the court seemed so unreceptive to the notion that privacy-invading speech may sometimes have a legitimate role in contributing to public debate was that in this case, the argument was very weak on the facts. In other words, while the German Courts rightly pointed out the important role of 'infotainment' in stimulating debate on matters of public concern in general, it was very hard to see just *what* topics might thus be stimulated through such anodyne photographs of Princess Caroline, still less why a ceaseless parade of such pictures was needed. Thus the Strasbourg court was arguably not confronted with any plausible argument as to the role of the particular pictures and articles concerned in stimulating public debate and thus did not need to engage with it. Paradoxically indeed, the very fact that the photographs were *not* particularly intrusive could also be said to be the reason why they contributed to no debate of general interest. In contrast, pictures of a celebrity emerging from a brothel, or a drug treatment centre, or an

[166] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at para. 64 (emphasis added).
[167] (1992) 14 EHRR 843.

abortion clinic, whilst more intrusive, could be argued *also* to make a contribution to a serious public debate – on prostitution, drug addiction, or abortion, as the case may be.[168] It would therefore be interesting to see how Strasbourg would respond to a case such as *Campbell*, in which the picture and articles in question, while clearly strongly engaging private life, also *did* relate to such a matter of serious public concern, as well as engaging the notion of the importance of the public's not being misled by previous untruthful statements by the applicant. However, its very partial and cautious upholding of press freedom in *Plon (Société)*, a case which, by any standards raised issues of public interest of immeasurably greater importance than the details of Campbell's treatment for drug addiction, would strongly suggest that had the Court of Appeal decision against her been the final one in domestic law, and Campbell had gone to Strasbourg, there would have been a resounding finding of breach of Article 8.

In contrast, it is clear that *all* the judges in the *Campbell* litigation were of the view that the press performed a legitimate function in the public interest in correcting the false impression Campbell had created as to her relationship with illegal drugs. Moreover, as is well known, much more flimsy public interest arguments than this have been accepted by English courts as a reason for overriding privacy claims. These include, notoriously, the notion that the immoral sexual behaviour of football players[169] or television presenters[170] were of legitimate public concern, because they were 'role models' for young people, while the fact that the Chair of Britain's Olympic bid team had had an affair has also been judicially determined to be a matter of legitimate public concern,[171] as, most recently, have been the marital problems of David and Victoria Beckham.[172] In short, English judges seem wedded to the notion that

[168] Sanderson makes a similar point, speculating whether the perverse outcome of *Von Hannover* may be to encourage journalists to uncover more disreputable facts relating to celebrities, in the hope of thereby being able to benefit from a more plausible 'public interest argument': Sanderson, 'Is *Von Hannover* v. *Germany* a Step Backward', above n. 119, 643–4. The decisions in *Tammer* v. *Estonia* (2001) 37 EHRR 857 and *Campmany Y Diez de Revenga* v. *Spain* (unreported, ECHR, no. 54224/00, 12 December 2000), however, would give little encouragement to such a course of action.

[169] *A* v. *B plc* [2003] QB 195.

[170] *Theakston* v. *MGN* [2002] EMLR 22.

[171] *Coe* v. *Mirror Group Newspapers* (Unreported, QBD, Fulford J, 29 May 2004).

[172] In a recent, unreported decision, the Beckhams were denied an injunction in relation to a story detailing problems within their marriage, including very intimate material, provided by their former nanny in clear breach of contract, apparently at least partly on the grounds of the 'public interest' of the story: see Owen Gibson, 'Celebrities Fear Revelations after Beckham Case Ruling', *The Guardian* (London), 25 April 2005, http://media.guardian.co.uk/site/story/0,14173,1471125,00.html.

information about the intimate private lives not only of politicians, but of various minor and major celebrities, may be of genuine public interest,[173] sufficient to override clearly weighty privacy claims. It seems tolerably clear from *Von Hannover* that the decisions in these cases take a view of the scope of the 'public interest' from which Strasbourg would strongly dissent. Clearer still are the indications from the decision of the court in *Campmany Y Diez de Revenga* v. *Spain*,[174] which, as noted above, concerned very similar facts to the cases just mentioned: sensational reportage of an affair between two persons of interest to the public, but who had no political or official role. In that case, the court found emphatically:

> Like the Spanish courts, the Court considers that as they concentrated on the purely private aspects of the life of those concerned and even though those persons were known to the public, the reports in issue cannot be regarded as having contributed to a debate on a matter of general interest to society.[175]

In this instance, the Strasbourg court's view appears the more compelling; however, as the analysis of *Von Hannover* discloses, the Strasbourg court's dismissal of reportage of private lives as a legitimate function of the press goes much, much further than this case. Arguably, Strasbourg takes an under-inclusive notion of the public interest, in which, seemingly, only the private lives of those who perform official duties can be of such legitimate concern, and then only exceptionally. Even then, the *Plon (Société)* case indicates that a high degree of protection for privacy can be afforded even to those who hold the highest political office,[176] while *Tammer* v. *Estonia* indicates that the sexual life of senior politicians can be wholly protected from publicity.[177] There does indeed appear to be a gulf in attitudes here, and, given that the *Beckham* decision was taken after *Von Hannover*, little sign that English courts are heeding this aspect of the

[173] See Markesinis et al, above n. 119, pp. 158–60; Gavin Phillipson, 'Judicial Reasoning in Breach of Confidence Cases under the Human Rights Act: Not Taking Privacy Seriously?' [2003] *European Human Rights Law Review* (Privacy Special) 53 at 60–72.

[174] (Unreported, ECHR, no. 54224/00, 12 December 2000.) It concerned what was described in the Spanish media as 'a new sex scandal between an attractive aristocrat and a banker from this country', including pictures and details of their tryst.

[175] Ibid.

[176] In that the interim injunction in that case was found not to violate Article 10.

[177] (2001) 37 EHRR 857 at para. 59. In that case, the court found that penalties imposed by the national authorities upon the reporting of an affair between the former Prime Minister and a former political aide were not a violation of Article 10.

Strasbourg jurisprudence. It may be said that English courts are too ready to accede to flimsy 'public interest' arguments in privacy cases, whilst Strasbourg arguably goes to the opposite extreme.

Conclusion

The House of Lords decision in *Campbell* has given English law a privacy tort; more precisely a cause of action in respect of the misuse of personal information. Whether English judges continue to refer to it as 'breach of confidence' or more boldly, recognise that 'the law of confidence . . . like a mother swollen with the child of privacy . . . [has] given birth and the umbilical cord cut'[178] may be a matter of semantics only. The new tort consists of two elements: facts in relation to which there is a reasonable expectation of privacy, and unauthorised use of those facts. Once that threshold is crossed, the court moves directly to balancing the privacy interest with the competing expression rights of the press, an exercise driven by the Convention. Since the test of 'reasonable expectation of privacy' was that used very recently by the court in *Peck* v. *UK*, it may in fact be said that, while we notionally have only indirect application of Article 8 through the common law action of confidence, the position arrived at is more or less the same as it would have been had Article 8 and its associated jurisprudence been directly applied by the courts.

Whether the newly created English privacy tort goes as far as the decision in *Von Hannover* is, as discussed, highly debatable. This chapter has discussed an interpretation of the latter that renders it considerably less absolutist in its demands on national privacy laws and it is to be anticipated that some such reading of *Von Hannover* will be adopted by the English courts as a means of reconciling that decision with *Campbell*. Finally, while the English courts have now settled upon a proper means of approaching the adjudication between Articles 8 and 10, and there is agreement that the contribution of a given story to a debate of genuine public interest is the crucial question, a gulf seems to have opened up between English and Strasbourg conceptions as to what types of 'private fact' *can* make such a contribution. While English courts have been rightly criticised for swallowing flimsy press arguments of 'public interest', Strasbourg is in danger of adopting a rigid and artificial distinction between facts relating to politicians and those with official functions on the one

[178] These dicta are from the initial judgment of Jack J in *A* v. *B* (unreported, QBD, 30 April 2001) at 16–17.

hand and everyone else on the other,[179] thus taking insufficient account of the enormous influence that nominally private actors can have on contemporary society. A compromise between the two positions is needed: one that is realistic in its appreciation of the importance of such influence and of the valuable role that 'infotainment' reportage *can* play in stimulating public debate, but rigorous in scrutinising claims that reportage of private facts will have this effect and, on the particular facts of the case, is a necessary and proportionate means of doing so.

[179] Sanderson, for example, argues that the *Von Hannover* decision wholly fails to recognise an intermediate category, *between* public officials and private citizens, of influential public figures: Sanderson, 'Is *Von Hannover* v. *Germany* a Step Backward', above n. 119, 636–9.

9

Privacy and constitutions

KENNETH J. KEITH

The prescription for the speech, on which this chapter is based, asked: what differences do constitutions make to privacy protection? As someone well versed in the practical implications of constitutions, the notice continued, I was to address the question from an international and comparative perspective. I wondered about this claim but I then thought I should draw on various parts of my professional experience, as a public servant, academic, law reformer and judge.

As a legal officer in the New Zealand Department of External Affairs over forty years ago, I analysed the new Canadian Bill of Rights against the proposal for a New Zealand equivalent and I had a hand in the formulating of New Zealand's position on some of the provisions of the draft International Covenants on Human Rights. Next, later in the 1960s, when I was a junior academic at Victoria University of Wellington, human rights issues were prominent in the Law Faculty's public law and international law teaching and writing, including a published series of lectures given in the 20th anniversary year of the Universal Declaration of Human Rights.[1] When I sat as a part-time judge for the first and second times, about twenty years ago, it was in difficult constitutional cases in the Pacific in which legislation was challenged as being in breach of constitutional

This chapter is based on an address I gave at the Centre for Media and Communications Law, University of Melbourne on 16 October 2003, a few hours before the House of Lords gave its judgment in *Wainwright* v. *Home Office* [2004] 2 AC 406 and while the judgment of the New Zealand Court of Appeal in *Hosking* v. *Runting* was reserved; see now [2005] 1 NZLR 1. I am grateful for the comments on my oral presentation made by Professor Geoffrey Lindell and Justice Michael Kirby, and by a referee on a draft of the chapter.

[1] See Kenneth Keith (ed.), *Essays on Human Rights* (Wellington: Sweet & Maxwell, 1968); for a seminar, another thirty years on, 'Seminar Commemorating the 50th Anniversary of the Universal Declaration of Human Rights' (proceedings) (1999) 29 *Victoria University of Wellington Law Review* 27 and (1998) 4 *New Zealand Association for Comparative Law* 27.

guarantees of equal protection of the laws.[2] That experience, I might say, made me wonder whether judges should be left with such broad standards against which to test the validity of legislation duly enacted by parliament and it affected the advice I gave to the Minister of Justice a little later on a Bill of Rights for New Zealand.[3] As a member of the Committee on Official Information, the Law Commission and the Legislation Advisory Committee I also addressed various aspects of the legislative protection of privacy.[4] And privacy issues arise in a range of court contexts, including the law of search and seizure and the suppression of the publication of aspects of court process.[5]

In New Zealand we now have over ten years of experience of a statutory Bill of Rights. Even if it is not a constitutional bill, it does present some of the same challenges as an entrenched bill, and raises the question about the difference the form and force of the legal instrument makes. Relevant to that question is the relationship between the national and the international in human rights matters. To take the specific matter of privacy, both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR) affirm in almost identical terms that:

[1] No one shall be subjected to arbitrary [or unlawful] interference with his privacy, family, home or correspondence, nor to [unlawful] attacks upon his honour and reputation.

[2] *Saipa'ia Olomalu* v. *Attorney-General* (1982) 14 *Victoria University of Wellington Law Review* 275, WS CA; *Clarke* v. *Karika* (1983) 2 Cook Islands judgments 102; [1985] LR Com (Const) 732, CI CA. The role of constitutional lawyers in the Pacific (and indeed beyond) is much wider than the adjudicative of course. See, e.g., Colin C. Aikman, 'Recent Constitutional Changes in the South-West Pacific' in *1968 New Zealand Official Yearbook* (Wellington: Government Printer, 1968) p. 1104; Alison Quentin-Baxter, 'Making Constitutions, from the Perspective of a Constitutional Advisor' and Alex Frame, 'Lawyers and the Making of Constitutions: Making Constitutions in the South Pacific' in David Carter and Mathew Palmer (eds.), *Roles and Perspectives in the Law: Essays in Honour of Sir Ivor Richardson* (Wellington: Victoria University Press, 2002) pp. 239 and 277; also published in (2002) 33 *Victoria University of Wellington Law Review* 661 and 699.

[3] See, e.g., Kenneth Keith, 'Democracy and a Bill of Rights for New Zealand? Judicial Review versus Democracy?' (1985) 11 *New Zealand Universities Law Review* 307. No provision on privacy was included in the draft Bill as proposed in 1985 or in the Bill as enacted: see *Hosking* v. *Runting* [2005] 1 NZLR 1 at paras. 22, 91–6 and 181.

[4] New Zealand, Committee on Official Information, *Towards Open Government: General Report* (Wellington: Government Printer, 1980); Committee on Official Information, *Towards Open Government, Supplementary Report* (Wellington: Government Printer, 1981) and, e.g., Legislation Advisory Committee, *Report No. 8* (Wellington: New Zealand Department of Justice, 1994) paras. 29–48 and 73–91.

[5] E.g. *R.* v. *Liddell* [1995] 1 NZLR 538; *R.* v. *Grayson and* Taylor [1997] 1 NZLR 399; *Television New Zealand Ltd* v. *R.* [1996] 3 NZLR 393 and *Re Victim* [2003] 3 NZLR 220.

[2] Everyone has the right to the protection of the law against such interference or attacks.[6]

(The Covenant provision includes the bracketed words.)

Australia, like New Zealand and the other 150 parties to the Covenant, is accordingly obliged to recognise a right to privacy in its law. That international obligation is to be compared with the obligation arising from a national bill of rights, even an entrenched one. For one thing the international obligation is apparently binding forever[7] while national constitutions are subject to alteration even if the process is a difficult one.

* * * *

In a recent analysis of 'the legal protection of the face we present to the world' Judge Richard A. Posner suggests that economics, a bit of simple game theory and some help from philosophy can help us think concretely about problems often obscured by what he refers to as sonorous talk of 'privacy'.[8] Jonathan Franzen, a notable American novelist and essayist, is blunter:

> The right to privacy – defined by Louis Brandeis and Samuel Warren, in 1890, as 'the right to be let alone' – seems at first glance to be an elemental principle in American life. It's the rallying cry of activists fighting for reproductive rights, against stalkers, for the right to die, against a national health-care database, for stronger data-encryption standards, against paparazzi, for the sanctity of employer e-mail, and against employee drug testing. On closer examination, though, privacy proves to be the Cheshire cat of values: not much substance, but a very winning smile.
>
> Legally, the concept is a mess. Privacy violation is the emotional core of many crimes, from stalking and rape to Peeping Tommery and trespass, but no criminal statute forbids it in the abstract.[9]

He goes on to discuss the relevant civil law, referring to it as a 'crumbly set of torts'.

[6] Universal Declaration of Human Rights, GA Res 217A, 3 UN GAOR (183rd plen mtg), UN Doc A/Res/217A (10 December 1948), Art. 12; and International Covenant on Civil and Political Rights, opened for signature 19 December 1966, 999 UNTS 171, 6 ILM 368 (entered into force 23 March 1976), Art. 17.

[7] E.g., Kenneth J. Keith, 'A Bill of Rights: Does It Matter?' (1997) 32 *Texas International Law Journal* 393.

[8] Richard A. Posner, 'The Legal Protection of the Face We Present to the World' in *Overcoming Law* (Cambridge, Mass.: Harvard University Press, 1995) pp. 531–51.

[9] Jonathan Franzen, 'The Imperial Bedroom' in *How to be Alone* (London: Harper Collins, 2002) pp. 42–3. I discuss the Warren and Brandeis article later in this chapter.

One way of thinking concretely and getting beyond the fading cat is to identify different situations where the word 'privacy' is used. There is a danger, against which Geoffrey Palmer when a professor at Victoria University of Wellington valuably warned over thirty years ago, in lumping together too many disparate topics under a single heading.[10] The case can be made that he failed to act on that sensible position when he was the minister responsible for introducing the very broadly applicable New Zealand privacy legislation, but I will not go down that track here. Rather, drawing on his and others' lists, I identify three of the many areas of law often captured under the head of privacy. I will make a substantive comment or two under each and conclude by referring to processes for the making and application of the law in those and related areas.

I consider

- powers of search and seizure, especially in this time of developing technology and the 'campaign against terror';
- the giving of publicity to private facts; and
- the criminalisation by the state of private acts.

Powers of search and seizure

In the sixth year of the reign of George III, four years before Captain James Cook made landfall in New Zealand, Lord Chief Justice Camden, in the Court of Common Pleas, decided the 'Case of Seizure of Papers' in favour of John Entick, clerk, against Nathan Carrington and three other messengers in ordinary to the King.[11] The statement of claim was

> In trespass; the plaintiff declares that the defendants on the 11th day of November in the year of our Lord 1762, at Westminster in Middlesex, with force and arms broke and entered the dwelling-house of the plaintiff in the parish of St Dunstan, Stepney, and continued there four hours without his consent and against his will, and all that time disturbed him in the peaceable possession thereof, and broke open the doors to the rooms, the locks, iron bars, &c. thereto affixed, and broke open the boxes, chests, drawers, &c. of the plaintiff in his house, and broke the locks thereto affixed, and searched and examined all the rooms, &c. in his dwelling-house, and all the

[10] Geoffrey Palmer, 'Privacy and the Law' [1975] *New Zealand Law Journal* 747; see also James Michael, 'Privacy' in David Harris and Sarah Joseph (eds.), *The International Covenant on Civil and Political Rights and United Kingdom Law* (Oxford: Clarendon Press, 1995) pp. 333–54.

[11] *Entick* v. *Carrington* (1765) 19 St Tr. 1029.

> boxes, &c. and so broke open, and read over, pried into and examined all the private papers, books, &c. of the plaintiff there found, whereby the secret affairs, &c. of the plaintiff became wrongfully discovered and made public; and took and carried away 100 printed charts, 100 printed pamphlets, &c. &c. of the plaintiff there found, and other 100 charts, &c. &c. took and carried away, to the damage of the plaintiff 2,000*l*.[12]

The defence among other things pleaded that the plaintiff was involved in the writing of 'very seditious papers containing gross and scandalous reflections and invectives upon His Majesty's Government and both Houses of Parliament'.

Defences based on legislation failed and Lord Camden turned to the final issue which he formulated in this way:

> . . . if this point should be determined in favour of the jurisdiction, the secret cabinets and bureaux of every subject in this kingdom will be thrown open to the search and inspection of a messenger whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel.[13]

Having thus described the very wide extent of the power Lord Camden continued in a passage which has become famous:

> Such is the power, and therefore one should naturally expect that the law to warrant it should be clear in proportion as the power is exorbitant.
>
> If it is law, it will be found in our books. If it is not to be found there, it is not law.
>
> The great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole. The cases where this right of property is set aside by positive law, are various. Distresses, executions, forfeiture, taxes, &c. are all of this description; wherein every man by common consent gives up that right, for the sake of justice and the general good. By the laws of England, every invasion of private property, be it ever so minute, is a trespass . . .
>
> The justification is submitted to the judges, who are to look into the books; and if such a justification can be maintained by the text of the statute of law, or by the principles of common law. If no such excuse can be found or produced, the silence of the books is an authority against the defendant, and the plaintiff must have judgment.

[12] Ibid. 1030. [13] Ibid. 1063.

> According to this reasoning, it is now incumbent upon the defendants to shew the law, by which this seizure is warranted. If that cannot be done, it is a trespass.
>
> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.[14]

The state must therefore have legislative authority if it is to search another's property and to seize it. But constitutional law and principle have a further role to play in relation to any proposed grant of that authority. Principles concerning the conferral of such powers, their extent, and controls over their exercise have been developed down the years by law reform agencies and others.[15] That work is just one reminder of the role of legislatures and those advising and influencing them in protecting human rights.

In addition to very extensive legislative practice and the principles stated by law reform bodies and in Article 17 of the ICCPR, in New Zealand's case there is s. 21 of the New Zealand Bill of Rights Act 1990:

> s. 21 Unreasonable search and seizure
> Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

That provision was as far as the drafters of the Bill of Rights were willing to go in recognising the right of privacy in that instrument, notwithstanding the broader terms in Article 17.[16] There has also been no move to broaden

[14] Ibid. at 1065–6.

[15] See, e.g., the Legislation Advisory Committee, *Legislative Change: Guidelines on Process & Content* (Wellington: New Zealand Department of Justice, 1991), paras. 48–142 and the earlier Law Reform Committee report on which the Court of Appeal depended in the *Choudry* case, discussed later.

[16] Minister of Justice, *A Bill of Rights for New Zealand – A White Paper* (1985) Appendices to the Journal of the House of Representatives, A 6 para. 10.144.

it notwithstanding the comments of the Human Rights Committee, the monitoring body set up under the ICCPR (to which I will return).[17]

That provision presents a number of important practical questions for police powers and criminal trials. I make one comment on each of two questions. What influence should that provision have on the interpretation of search powers conferred in particular statutes? And if evidence is obtained in breach of s. 21 on what basis, if any, should it be admitted?

The first question arose in a case about the powers of the New Zealand Security Intelligence Service (SIS) when acting under a ministerial warrant to intercept or seize a communication for security reasons.[18] Did that power extend to entering property covertly? The High Court said Yes. The Court of Appeal said No, using the Bill of Rights in a confirming, supportive role. The New Zealand Security Intelligence Act 1969 in its terms did no more than to empower the SIS to intervene in the communication process and acquire or seize information. There was nothing in the carefully structured language and scheme to justify going beyond that narrow grant of invasive powers. Nor was justification to be found in the report leading to the legislation, prepared by the Chief Ombudsman, Sir Guy Powles. Next, the Australian, Canadian and United Kingdom legislation all made express provision for entry:

> Those statutes recognise the important constitutional consideration that at common law every invasion of private property is a trespass and any intended erosion of the protection of the common law should be spelt out in the plainest terms as has been done in numerous statutes. Expressing the same concern for fundamental values, the Public and Administrative Law Reform Report 1983, para 3.08 concluded:
>
> 'In our opinion the conferring of a power to enter private property is too great an infringement of private rights to be done by implication. Parliament should give specific consideration to the need for it, and its intention to authorise such an interference deserves to be expressed by clear words.'[19]

The court then mentioned the Bill of Rights, as I have said, in a supporting role:

[17] United Nations, Human Rights Committee, *Concluding Observations of the Human Rights Committee: New Zealand*, CPR/CO/75/NZL, 26 July 2003, available at http://www.humanrights.co.nz/docs/HRC_concluding_observations02.doc, para. 8.

[18] *Choudry* v. *Attorney-General* [1999] 2 NZLR 582.

[19] Ibid. 592–3.

> Section 21 of the Bill of Rights, in conferring the right to be secure against unreasonable search and seizure, reflects those same values and concerns.[20]

I have to report that parliament in response to that decision conferred an express power of entry,[21] but the government of course had to justify that action in the face of the court's judgment and the principles on which the judgment was based.

On the admissibility issue, there is of course a huge amount of writing by judges and others. A New Zealand Court of Appeal of seven judges recently added to it.[22] I mention only one matter, to emphasise again the international context in which these matters must increasingly be seen. The multilateral human rights treaties do not, with only one exception, purport to regulate expressly the admissibility of evidence obtained in breach of them. Rather it is left for each state party to determine the appropriate legal remedy.[23] The exception is to be found in the Convention against Torture,[24] Article 15 of which prohibits the use as evidence of any statement made as a result of torture. That prohibition, it will be seen, does not extend to real or non-confessional evidence.

The established principles and rules face challenges as new technologies develop and as the public interest requiring powers of search is seen to change – as at present in the 'campaign against terror'.

Again one comment on each. On 11 June 2001 the United States Supreme Court decided that the use by the police of a heat-imaging device at a private home from a public street to detect relative amounts of heat within the house was a search. It was accordingly subject to the Fourth Amendment to the US Constitution. The heat was emanating from a marijuana operation within the house. The use of a device that is not in general public use to explore details of a private home that would previously have been unknowable without physical intrusion was held to be a search. The decision turns on the subjective expectation of privacy. At the very core of the Fourth Amendment 'stands the right of a man to retreat into his own house and there be free from unreasonable governmental intrusion'.[25]

[20] Ibid. 593.

[21] New Zealand Security Intelligence Service Act (1969), ss. 4B–4K as enacted in 1999 and amended in 2003.

[22] *R.* v. *Shaheed* [2002] 2 NZLR 377.

[23] See, e.g., Art. 2(3)(a) as well as Art. 17(2) of the ICCPR.

[24] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, opened for signature 10 December 1984, 1465 UNTS 85 (entered into force 26 June 1987).

[25] *Silverman* v. *US*, 365 US 505 at 511 (1961).

To decide otherwise said the court, would leave the homeowner at the mercy of advancing technology, including imaging technology that could discern all human activity in the house. This was more than a naked eye search from a public street of the exterior of the house. The dissenters by contrast said that the use of the device was an 'off-the-wall' observation rather than a 'through-the-wall' surveillance.[26]

The measures taken by states since 11 September 2001 to meet the challenges of terrorism, in part at least in response to binding obligations arising from United Nations Security Council Resolution 1373,[27] are already the subject of an avalanche of commentary. Again, I refer to one matter in support of the proposition that we must take care in times of peril not to endanger that which is essential to our system of constitutional and democratic government under the rule of law. That one matter is the international supervision which now exists regionally and internationally over the taking of emergency measures, many of them involving threats to privacy.

The Human Rights Committee in its most recent comment on New Zealand's periodic report under the ICCPR has expressed its concern that the impact of New Zealand's measures under resolution 1373 on its obligations under the Covenant may not have been fully considered.[28] (It also repeats its concern that the Bill of Rights is an ordinary statute, subject to repeal.)[29] Its statement of concern on the United Kingdom's proposed measures is stronger.[30] Those comments are not binding but responsible governments must obviously consider them seriously and in good faith. They will be expected to respond to the comments in their next reports if not before.

The giving of publicity to private life

The law of search and seizure is essentially about the powers of the state to invade our privacy. I now turn to an area of law which operates primarily between individuals or in practice between individuals and the media. To take in a brief form the facts of a case decided by the New Zealand

[26] *Kyllo* v. *US*, 533 US 27 (2001). [27] 28 September 2001.
[28] *Concluding Observations of the Human Rights Committee*, above n.17, para. 11.
[29] Ibid. para. 8.
[30] See United Nations, Human Rights Committee, *Concluding Observations of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland*, CCPR/CO/73/UK, CCPR/CO/73/UKOT, 6 December 2001, available online from http://www.unhchr.ch, para. 6.

Court of Appeal in early 2004: the parents of young children wished to obtain an injunction to prevent a magazine publishing photographs of those children taken without the parents' knowledge and consent in a public street. Is there a tort of privacy which provides protection in such situations and if so does it provide for relief in this case? The court by three to two decided that there was such a tort but was unanimous that the claim failed on the facts. I was on that court and it would be wrong for me to enter into the substance of the case, but I may mention some of the relevant sources and issues of legal process which arise in such cases.[31]

To begin almost at the beginning, over one hundred years ago, we have Samuel Warren and Louis Brandeis in their famous article responding to Boston's yellow press.[32] I say almost at the beginning because they do draw on such crumbs of authority as they could find, beginning with the general proposition of Willes J that:

> It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage.[33]

They do not note that the claim in that case for a right under the common law to copyright failed, with the court holding that authors were secured in their copyright only under the Statute of Anne (8 c. 19). Willes J's broad proposition may also be compared with the requirement of Lord Camden, his contemporary, that authority for limits on freedom has to be found in the 'books'.

Warren and Brandeis also relied on the case about Prince Albert's etchings in which the proposed publication was condemned in fine Victorian rhetoric not only on the grounds of property, but also 'because it was an intrusion . . . not alone in breach of conventional rules, but offensive to that inbred sense of propriety natural to every man – if intrusion, indeed, fitly describes a sordid spying into the privacy of domestic life into the home (a word hitherto sacred among us), the home of a family whose life and conduct form an acknowledged title, although not their only unquestionable title, in the most marked respect in this country'.[34]

[31] *Hosking* v. *Runting* [2005] 1 NZLR 1. On sources, the 4 judgments refer to 21 statutes from 4 jurisdictions, 32 New Zealand court and tribunal decisions, 80 decisions from 6 other jurisdictions, 4 treaties and 19 other authorities; for legal process issues see, e.g., paras. 2–7, 87–97, 109–16, 177, 181 and 202–7 of the reasons, and the final part of this chapter.

[32] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

[33] *Millar* v. *Taylor* (1769) 4 Burr 2303 at 2312; 98 ER 201 at 206.

[34] *Prince Albert* v. *Strange* (1849) 2 De G & Sm 652 at 698; 64 ER 293 at 313.

It is interesting that over 150 years ago the protection of privacy as well as the protection of property is given in support of recovery.

The tort of giving publicity to private life as it exists in the United States is essentially the product of that great article and of the diligent work of counsel, judges and scholars over the decades since. Dean William Prosser is a major figure in this development, as is the American Law Institute (ALI). The Institute captured the tort in these words in 1976:

> 652D. Publicity Given to Private Life
> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicised is of a kind that
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public.[35]

With one exception (to which I will return) the impact of that text and the body of learning supporting it beyond the United States has so far been limited. It appears to have come into UK law not directly but rather by way of a recent Australian case where a privacy argument failed since the plaintiff meat processing company could not show that the information in question had the quality of privacy to it and that the fundamental values of personal autonomy were engaged. In his judgment Gleeson CJ used the ALI's words when he said that:

> The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.[36]

That passage was used in the leading English cases involving in one case Naomi Campbell, the supermodel, and in another a Premier League footballer.[37] This is an interestingly circuitous route for introducing privacy into the law of the United Kingdom, given that since 2 October 2000 its Human Rights Act 1998 has recognised in a direct form 'the right to respect for [an individual's] . . . private life' and neither Australian nor, for the most part, the US jurisdictions have such legislation. One recent careful review of the UK law laments the continuing dominance of the law of confidentiality, and the failure of the courts to appreciate that they

[35] See also William L. Prosser, 'Privacy' (1960) 48 *California Law Review* 383.
[36] *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at 226.
[37] *Campbell* v. *MGN Ltd* [2003] QB 633 at paras. 48–58, CA; and [2004] 2 AC 457 at paras. 93–4, 100 and 135, HL; and *A* v. *B plc* [2003] QB 195, CA.

are now faced with a direct clash between two rights – freedom of expression and the right to privacy. On this view, the courts have made things worse by raising freedom of expression to the status of a genuine constitutional right. Further, the courts should be recognising that some of the speech they are protecting is of the lowest value in European Convention terms.[38]

The relative insignificance of the Convention right to privacy in the law of the United Kingdom, at least to the present, is matched by the limited impact of the statutes creating general privacy torts in a number of US states and Canadian provinces. Those statutory measures appear to have had no significant effect at all over the several decades they have been in force.[39]

Another interesting thing about this body of law, to revert to the constitutional question, is that over the past one hundred years of the development of the Warren/ Brandeis/Prosser/ALI tort, the US Supreme Court has essentially avoided the First Amendment issues that a privacy right might be expected to present. It has expressly saved the question whether truthful publication of very private matters unrelated to public affairs could be constitutionally proscribed.[40] In the case in which it said that the court refused to hold unconstitutional a state law preventing the publication of a rape victim's name, it held that the state may not, consistently with the First and Fourteenth Amendments, impose sanctions on the accurate publication of a rape victim's name obtained from judicial records that are maintained in connection with a public prosecution and that themselves are open to public inspection. The protection of freedom of the press provided by the First and Fourteenth Amendments barred Georgia from making the appellant's broadcast the basis of civil liability in a cause of action for invasion of privacy that penalises pure expression – the content of a publication.[41] Further, the commission of a crime and prosecution and judicial proceedings resulting from it are events of legitimate concern to the public and fall within the press responsibility to report the operations of government.

That case involved the open justice principle which can often come into conflict with considerations of privacy. In a recent case, the New Zealand Court of Appeal agreed with the trial court judge's decision to lift the

[38] Gavin Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726.

[39] See *Hosking* v. *Runting* [2005] 1 NZLR 1 at paras. 216 and 219 and the sources referred to there and at paras. 74–5.

[40] *Cox Broadcasting Corp.* v. *Cohn*, 420 US 469 at 491 (1975).

[41] Ibid. 487–97.

suppression of the name of the alleged victim of a conspiracy to kidnap. The court began with the principle of open justice:

> The principle is long and well established, as Joseph Jaconelli valuably demonstrates in his *Open Justice: a critique of the public trial* (2002). He discusses the important reasons and values supporting the principle. They include the discipline placed by publicity on the participants in the justice process, including the judges, counsel and witnesses and particularly the accuser in criminal trials; the possibility that further witnesses will come forward; the facilitating of the attendance of the public with advantages in terms of observing the law being properly applied and administered, their legitimate interest in seeing charges of alleged offences against the whole community being authoritatively determined, and the deterrent thrust of the criminal law; and more broadly in the words of Lord Atkinson in the leading case of *Scott v Scott* [1913] AC 417, 463, that, although the hearing of a case in public may be and often is painful and humiliating, 'all this is tolerated and endured, because it is felt that in public trial is to be found, on the whole, the best security for the pure, impartial and efficient administration of justice, the best means for winning for it public confidence and respect'. The principle is of course not absolute.[42]

The court later recorded that it has consistently adopted the position of open justice, both before and after the enactment of the Bill of Rights: as in the SIS case, the Bill plays a confirming supporting role. The *Scott* reference does highlight the changing public judgments, at least as made by parliament, about what court processes should be closed. While in 1913 it was contrary to public policy for a divorce trial to be held in secret, legislatures have increasingly required that they be held in private.

I return to the exception to the proposition that the ALI text has had no real impact beyond the United States. The exception is New Zealand where the Court of Appeal essentially adopted it in recognising a tort of privacy.[43] This action presents an interesting contrast with that taken in the United Kingdom in constitutional terms. A right to privacy is part of UK law by virtue of the adoption of the European Convention on Human Rights through the Human Rights Act 1998 while the New Zealand Bill of Rights does not include a right to privacy, a decision deliberately taken, and yet the British courts have struggled with the adoption of a distinct tort of breach of privacy while the New Zealand courts have adopted it.

[42] *Re Victim X* [2003] 3 NZLR 220 at para. 5.

[43] *Hosking* v. *Runting* [2005] 1 NZLR 1 at paras. 117–28; cf. paras. 255–8; see also paras. 209–10.

The British courts' position may be seen as the more surprising given the direct application of the privacy article of the Convention by the European Court of Human Rights, for instance in the recent case brought by Princess Caroline of Monaco.[44] That is to say, constitutional texts may leave courts with considerable freedom in this area of rights as in others. We shall see something of that freedom in the US jurisprudence considered in the next part of this chapter.

State criminalisation of private acts

I am concerned under this heading not with Nathan Carrington and the three other messengers in ordinary to the King breaking into a house to undertake a wide ranging search, but with actions of the state that go further especially, but not solely, through the application of criminal law. The basic idea I am concerned with was stated in these words by Justice Kennedy in June 2003 at the beginning of an opinion of the US Supreme Court:

> Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct. The instant case involves liberty of the person both in its spatial and more transcendent dimensions.[45]

The court struck down a Texan statute making it a crime for two persons of the same sex to engage in certain intimate sexual conduct. To reach that conclusion they overruled an earlier decision. Three judges dissented, Justice Scalia speaking for them in his typically vigorous way and beginning with what he saw as the court's 'surprising' readiness to reconsider a decision rendered a mere seventeen years earlier.

I will come back to aspects of the reasoning in that case, but first I recall the debates about law and morality between those great Victorians, John Stuart Mill and James Fitzjames Stephens. Much the same debate arose in the United Kingdom and elsewhere following the publication in 1957 of the Wolfenden report, particularly in the exchanges between (Professor)

[44] *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at paras. 50–80; see also the case about the late President Mitterand, *Plon (Société)* v. *France* (unreported, ECHR, no. 58148/00, 18 May 2004); and consider s. 2(1) of the Human Rights Act 1998 (UK).

[45] *Lawrence* v. *Texas*, 539 US 558 at 562 (2003).

H. L. A. Hart and (Lord) Patrick Devlin.[46] That report, to the surprise of the Home Secretary, David Maxwell Fyfe who called for it, proposed that homosexual behaviour between consenting adults should no longer be a criminal offence. It was another ten years before that proposal became law in the United Kingdom and legislatures in this part of the world took even longer, with the New Zealand legislation being passed only in 1986.[47]

The chair of the committee, Sir John Wolfenden, it has been said, personally abhorred homosexuality: he thought it was a disgusting abomination. But he could not find any respectable reason for a government to interfere with the private behaviour of its adult citizens – a victory for intellectual process over personal distaste. Sebastian Faulks, whom I am quoting, adds a fascinating footnote to the previous part of this chapter on giving publicity to private facts. Sir John's son, Jeremy was 'devotedly' homosexual. 'It is difficult,' says Faulks writing in 1996, 'to imagine more than forty-eight hours lapsing in today's press before the first story – 'Vice Man's Son is Gay' – appeared in print. Jeremy had never made a secret of his sexual life; he was a famous figure in the small world of Oxford, and an active one in the larger sphere of London: his preferences were known about by hundreds, perhaps thousands of people.'[48]

I return to the constitutional aspects and in particular to the due process clause of the Fourteenth Amendment, seen at different times and in different ways as protecting substantive liberty, a deeply controversial area raising questions about the role of judges in a democracy. Should they, instead of elected legislators, for instance make decisions, as they have, about the availability of contraceptives to married couples, to the non-married and to persons under sixteen years of age, or the availability of abortion, or about class based legislation aimed at homosexuals, or about the criminality of private consenting sexual activity? If so, by reference to what tests? The constitutional provision says only that 'no state shall . . . deprive any person of life, liberty or property, without due process of law'. While privacy guarantees in the ICCPR and elsewhere are broad in their wording, they do give some greater sense of meaning than does the

[46] United Kingdom, Committee on Homosexual Offences and Prostitution, *Report of the Committee on Homosexual Offences and Prostitution* (London: HMSO, 1957); for a discussion of the exchanges see, e.g., Nicola Lacey, *A Life of H. L. A. Hart: The Nightmare and the Noble Dream* (Oxford: Oxford University Press, 2004).

[47] The change of the law in Tasmania was the result of a complaint to the Human Rights Committee, filed the day Australia became bound by the First Additional Protocol to the ICCPR allowing such complaints to be made: *Toonen* v. *Australia* (4/4/94) CCPR/C/50/D/488/1992.

[48] Sebastian Faulks, *The Fatal Englishman* (London: Random House, 1996) p. 241.

Fourteenth Amendment. Further, as Justice Scalia points out, some of the earlier decisions depended not on substantive due process but on the right to privacy, found in so-called penumbras of other constitutional provisions, and on equal protection – again heavily disputed matters. And to what material should the judges have regard in giving content to those provisions and principles?

On that last question, the Supreme Court depended on state legislation in the United States and its evolution, especially over the preceding seventeen years, the Wolfenden report, a 1981 decision of the European Court of Human Rights holding Irish legislation forbidding consensual homosexual activity to be in breach of the European Convention, later decisions to the same effect and legislative changes in other countries. It also returned to broad ideas of personhood:

> These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State.[49]

Justice Scalia attacks much of the reasoning, including the sources. On the last, for him, foreign views are meaningless, indeed dangerous since his court should not impose foreign moods, fads or fashions on Americans.[50] He also attacks the reasoning of Justice O'Connor, one of the majority seventeen years earlier, for striking down the legislation under the equal protection clause. The basis for that reasoning was that the statute in issue in the earlier case also applied to heterosexual acts while the Texan one was restricted to homosexual acts.

Justice Scalia finally emphasises the basic issue of democratic legitimacy and the value of leaving regulation of the matter to the people through legislatures. One advantage

> is that the people, unlike judges, need not carry things to their logical conclusion. The people may feel that their disapprobation of homosexual conduct is strong enough to disallow homosexual marriage, but not strong enough to criminalise private homosexual acts – and may legislate

[49] *Lawrence* v. *Texas*, 539 US 558 at 574 (2003), quoting *Planned Parenthood of Southeastern Pa.* v. *Casey*, 505 US 833 at 851 (1992).

[50] For a similar division in the court about the use of foreign material, this time in relation to the death penalty for juveniles, see *Roper* v. *Simmons*, 543 US 551 (2005).

> accordingly. The court today pretends that it possesses a similar freedom of action, so that that we need not fear judicial imposition of homosexual marriage, as has recently occurred in Canada . . . At the end of its opinion – after having laid waste the foundations of our rational-basis jurisprudence – the court says that the present case 'does not involve whether the government must give formal recognition to any relationship that homosexual persons seek to enter.' . . . Do not believe it. More illuminating than this bald, unreasoned disclaimer is the progression of thought displayed by an earlier passage in the Court's opinion, which notes the constitutional protections afforded to 'personal decisions relating to *marriage*, procreation, contraception, family relationships, child rearing, and education,' and then declares that '[p]ersons in a homosexual relationship may seek autonomy for these purposes, just as heterosexual persons do.' . . . (emphasis added). Today's opinion dismantles the structure of constitutional law that has permitted a distinction to be made between heterosexual and homosexual unions, insofar as formal recognition in marriage is concerned. If moral disapprobation of homosexual conduct is 'no legitimate state interest' for purposes of proscribing that conduct, . . . and if, as the Court coos (casting aside all pretense of neutrality), '[w]hen sexuality finds overt expression in intimate conduct with another person, the conduct can be but one element in a personal bond that is more enduring,' . . . what justification could there possibly be for denying the benefits of marriage to homosexual couples exercising '[t]he liberty protected by the Constitution,' . . .? Surely not the encouragement of procreation, since the sterile and the elderly are allowed to marry. This case 'does not involve' the issue of homosexual marriage only if one entertains the belief that principle and logic have nothing to do with the decisions of this Court. Many will hope that, as the Court comfortingly assures us, this is so.[51]

Justice Thomas, joining Justice Scalia, was very brief. The law is uncommonly silly, he said. If he was a member of the Texas legislature he would vote to repeal it. But his duty is to decide cases agreeably to the Constitution and laws of the United States.

As the end of the Scalia opinion indicates, there is much more that could be said under this heading, for instance, about gay marriage, civil unions and ambulatory readings or amendment of legislation, covering a host of topics, to make them cover gay relationships.[52] I limit my comment to the broad and contested understanding of 'liberty' which that word in the Fourteenth Amendment at times attracts in claims based on privacy.

[51] *Lawrence* v. *Texas*, 539 US 558 at 604–5 (2003).
[52] See, e.g., *Quilter* v. *Attorney-General* [1998] 1 NZLR 523.

The *Lawrence* court based its opinion on broad statements of the substantive reach of the due process clause, particularly in cases about intimate sexual matters. The court, it recalled, had invalidated a state law prohibiting the use of contraceptive drugs and devices and counselling or aiding and abetting their use. The protected interest in that case it said was a right to privacy (found in the Bill of Rights); the court also emphasised the married relationship and the protected space of the marital bedroom.[53] The right to make certain decisions about sexual conduct extended as well to persons who were not married[54] and were under sixteen.[55] In the former it agreed with the appeals court that

> If the right of privacy means anything, it is the right of the *individual*, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.[56]

Although in *Roe* v. *Wade*,[57] the successful challenge to a Texan law prohibiting abortions, the court held that the woman's rights were not absolute, 'her right to elect an abortion did have real and substantial protections as an exercise of her liberty under the Due Process Clause'.

It was on the basis of such authority that the court asserted in the passage already quoted its broad concept of personhood. As already indicated it is strongly contested. For Justice Scalia the passage just quoted is a 'famed sweet-mystery-of-life passage', a passage capable of eating the rule of law. The authorities cited by the court, he says, do not lead to the conclusion it reached. The court moreover has taken sides in the culture war, departing from its role of assuring, as neutral observer, that the democratic rules of engagement are observed.[58]

Legal method

That dispute leads directly to matters of legal method, with which I conclude. How can lawyers and lawmakers best help in striking the balance

[53] *Griswold* v. *Connecticut*, 318 US 479 (1965). [54] *Eisenstadt* v. *Baird*, 405 US 439 (1972).
[55] *Carey* v. *Population Services International*, 431 US 648 (1977).
[56] *Eisenstadt* v. *Baird*, 405 US 439 at 453 (1972). [57] 410 US 513 (1973).
[58] This statement of role may be related to the thesis of John Hart Ely in *Democracy and Distrust: A Theory of Judicial Review* (Cambridge, Mass.: Harvard University Press, 1980), a thesis which influenced the preparation of the New Zealand Bill of Rights: see Keith, 'Democracy and a Bill of Rights for New Zealand?' above n. 3. For Ely the due process clause is about process, not substance; 'substantive due process', he says, is a contradiction in terms – sort of like 'green pastel redness' (p. 18).

between the right of the public to know and the right of the individual to be let alone? Which of the various actors and law making methods should strike that balance in particular cases?

Two methods of regulating privacy issues other than those I have mentioned should be added. The first is through voluntary industry and professional codes, such as those that advertisers, broadcasters and journalists might and in fact do adopt (a matter mentioned in *Hosking*).[59] While such codes sometimes have a statutory base, they more often are purely private, being based on contract and having an ethical force. The second is through international guidelines rather than treaties, such as the recommendations made by the Organisation for Economic Cooperation and Development twenty-five years ago which had a major impact on legislation in Australia and New Zealand.[60] As the ALI restatement shows at the national level, it is not always necessary to aim at a binding text.

I recall in a summary way five broad matters which are interrelated and which should have a central role in scholarly research, particularly in the universities.[61] The first is the available range of methods of law making and law application – national and international; private (or non-official) and public (or official); binding and recommendatory; constitutional, legislative, judicial and executive; and through commentary and public debate.

The second is the varying approaches of different institutions at different times to their authority and to the way they might exercise it; that is most apparent, you might think, in the work of judges, since they have to explain themselves and the explanations do sometimes extend into explicit discussions of judicial method. But consider the role of reform and review bodies, of professional bodies, of individual scholars and of the public philosophers such as John Stuart Mill or Richard Posner or Jonathan Franzen: because they do not decide but do or may hope to persuade, their reasoning may be even more important. That reasoning may address the question why they, rather than another, should be listened to, or why one lawmaker rather than another should have the responsibility for restating or developing the law.

Third is the very wide range of material, sources if you will, relevant to the task of the various decision makers I have been mentioning; there

[59] [2005] 1 NZLR 1 at paras. 166–8, 198–9 and 206.

[60] See the Privacy Act 1988 (Cth) and the Privacy Act 1993 (NZ) (the recommendations are referred to in the title).

[61] Compare the image of the four floors used by Charles Leadbeater in his preface to *Up the Down Escalator – Why the Global Pessimists are Wrong* (London: Penguin, 2003).

has for instance been something of a revolution in the information made available to and used by courts over the past forty or so years; but does that mean their function moves closer to that of a law reform agency?

That takes me to my fourth point: how are the choices to be made between the various methods of law making? Is not our approach to that rather haphazard? You might say that I am looking for greater system and order than is practicable or even desirable. We should however be aware of the choices. Is it not the task of the law, of the lawyer, especially in the university, to propose guidance for what at times appears to be a chaotic process of choice?

To illuminate those questions I conclude with another decision of the New Zealand Court of Appeal, this time about a witness in a criminal trial who wished to keep his name and address private.[62] The argument had to be made under the common law, there being no directly applicable legislation. The trial judge ruled that the witness could have that anonymity; the accused was convicted, and he appealed. Two judges in the Court of Appeal agreed with the trial judge, but the other three disagreed, set aside the conviction and ordered a new trial. The majority considered that on the material before the court they could not assess the gravity and extent of the problem raised by such witnesses and determine the appropriate response. The court would face obvious difficulties in fashioning a new common law rule. The matter was better handled through law reform and parliamentary processes – as indeed it was, in very short order.[63] The minority, by contrast, considered that the development of the law in this area fell properly within the judicial function.

The final reflection is about the significance for judges of the constitutional, or for that matter legal, status of the right in issue. The controversies in the United States about 'substantive due process', a phrase which might by its apparent contradiction alert the reader to the proposition that words matter, and the contrasting positions of the British and New Zealand judges – a contrast which appears to be the contrary to the positive law – show that the constitutional or statutory text is not all. Among the other significant matters are the principles and values underlying the law (or thought to) and (differing) understandings of the judicial role.

[62] *R.* v. *Hines* [1997] 3 NZLR 529.

[63] Evidence (Witness Anonymity) Amendment Act 1997 following a report of New Zealand's Law Commission, *Evidence Law: Witness Anonymity*, NZLC R42 (Wellington: Law Commission, 1997). Note the safeguards which parliament stated in the Act and which a court could not have created, including a ministry review of the operation of the Act after three years and automatic removal of the trial to the High Court if an anonymity order is made.

I am sure many judges would welcome greater guidance on the choices they are to make in cases such as those considered in this chapter. Thinking of those issues and of the path-breaking article on privacy which he co-authored, I end with Louis Brandeis and the tribute which Paul Freund paid to that great judge. The conclusion to that tribute does, I think, help us address those choices of law-making methods which Brandeis' own career as scholar, advocate, adviser and judge illuminates. His power, declared Freund,

> derived from a fusion of three traditions: the Biblical tradition, with the moral law of responsibility at the core; the classical tradition, with its stress on the inner check, the law of restraint, proportion, and order, achieved by working against a resisting medium; and not least, the common-law tradition teaching that life of the law is response to human needs, that through knowledge and understanding and immersion in the realities of life law can be made, in Mansfield's phrase, to work itself pure.[64]

[64] Paul A. Freund, 'Mr Justice Brandeis' (1957) 70 *Harvard Law Review* 769, reprinted in Paul A. Freund, *On Law and Justice* (Cambridge, Mass.: Belknap Press of Harvard University Press, 1968) p. 145.

10

Celebrity privacy and benefits of simple history

MEGAN RICHARDSON AND LESLEY HITCHENS

Introduction

Is personal revelation the right of the subject alone or can others tell the story even without consent? The question lies at the heart of recent celebrity privacy cases. When Michael Douglas and Catherine Zeta-Jones claimed their wedding party had been intercepted by underground paparazzi with the photographs to be published in *Hello!*, their complaint was not that they should be let alone completely. Indeed they had contracted with *OK!* to give the public account of their celebration with carefully vetted authorised pictures. Yet they claimed their privacy was implicated and the equitable action for breach of confidence was the way to protect this; a claim partly and with some reservations accepted by the courts, which refused an interlocutory injunction[1] but subsequently allowed damages for the unauthorised publication (at the time suggesting the injunction should have been awarded).[2] When Naomi Campbell found herself the subject of an article in the *Mirror* revealing details of her treatment for a drug addiction, with covertly taken photographs in support, her essential complaint was that the story had been obtained and published without her knowledge or approval (although conceding that her own previous false accounts meant she was in no position to prevent telling about her addiction). Further, the House of Lords left her the option in finding her confidence breached.[3] In the New Zealand case of *Hosking* v. *Runting*, where a tort of public disclosure of private facts was recognised

We are grateful to Andrew Kenyon for helpful comments and advice in the course of preparing this chapter.

[1] *Douglas* v. *Hello! Ltd* [2001] QB 967.

[2] *Douglas* v. *Hello! Ltd* [2006] QB 125, approving in part the decision of Lindsay J in *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996.

[3] *Campbell* v. *MGN Ltd* [2004] 2 AC 457.

(a doctrine rather similar to breach of confidence in other jurisdictions),[4] the Court of Appeal might have given a remedy against publication in *New Idea* of the defendant's surreptitious photographs of the normally self-publicising celebrity plaintiffs' family outing had the information been treated as private and confidential by the parties involved.[5] *Von Hannover* v. *Germany* involved a claim about Princess Caroline's entitlement to determine when aspects of her personal life should be told to the public through the press and when they should not – and although the European Court suggested the more serious violation of Article 8 of the European Convention on Human Rights[6] lay in the paparazzi's intrusive practices of constant surveillance, it also accepted this basic entitlement continued notwithstanding her celebrity status.[7]

The privacy claims in these cases seem far removed from the right to be 'let alone' talked of in classic texts.[8] Has the language of 'privacy' become a mask for protection of other interests not really to do with privacy at all – a de facto publicity right perhaps? Or is it rather that privacy can no longer, if ever it could, be simply about the right to be let alone? We contend the latter and, moreover, that the equitable breach of confidence doctrine is well-suited to embrace and sustain the controlled self-revelatory aspect of modern celebrity privacy cases. Nor should this surprise: early cases in which the doctrine was established were in subject matter, situations, themes, and even language more notable for their similarities with than differences from the recent cases.

Prince Albert v. *Strange*: a case study in celebrity privacy

The case of *Prince Albert* v. *Strange*[9] was, as Lord Cottenham LC said, distinguished more by the 'exalted station of the Plaintiff' than by any difficulty in the principle to be applied. Indeed, there were several.

[4] Especially those jurisdictions which accepted surreptitious obtaining as giving rise to a confidentiality obligation (a position New Zealand courts had ruled out): see Megan Richardson, 'Privacy and Precedent: The Court of Appeal's Decision in *Hosking* v. *Runting*' (2005) 11 *New Zealand Business Law Quarterly* 82.

[5] *Hosking* v. *Runting* [2005] 1 NZLR 1.

[6] Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952).

[7] *Von Hannover* v. *Germany* (2005) 40 EHRR 1.

[8] Most famously Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, who said 'the principle which protects personal writings and other personal products . . . against publication in any form, is in reality . . . a principle of inviolate personality': at 196–7.

[9] *Prince Albert* v. *Strange* (1849) 1 H & TW 1; 47 ER 1302.

Breach of trust and confidence

Breach of 'trust, confidence or contract' was an obvious basis for the grant of an injunction to prevent sales of a catalogue containing descriptions of family etchings which Queen Victoria and the Prince Consort had executed for private enjoyment[10] – at least once it was clear how the information had come into the hands of the defendant, William Strange. There was some doubt about this initially; as a result, discussion of trust and confidence featured little in the first instance judgment of Knight Bruce V-C.[11] However, it eventually emerged that copies of the etchings, entrusted to a printer for the purpose of having limited copies made for private circulation, had been passed by an employee of the printer to a journalist, Jasper Judge, who passed them to Strange for the purpose of mounting a public exhibition. The plan was abandoned once it was clear that royal permission would not be given, but Strange sought to publish the descriptive catalogue he had prepared so as to recover the costs incurred. He argued his innocence but as Lord Cottenham LC noted, he could 'not suggest . . . any mode by which [the etchings] could have been properly obtained'.[12] The facts as found were enough to find breach of a relationship of trust and confidence entered into with the printer, with liability extending to Judge and to Strange through the latter's tacit complicity in the wrongdoing. Even so, it was already clear by 1849 that there were many possible ways in which a person's private activities might be exposed to the world, ways which themselves might be secret and never fully disclosed.[13] Thus Lord Cottenham LC, taking a strand of authority suggested in *Abernethy* v. *Hutchinson* (a case similarly unclear as to the precise origins of the unauthorised publication),[14] referred to the wrongful 'surreptitious' character of the obtaining by Judge; a wrong

[10] The etchings which dated back to 1840 and were signed as being by Queen Victoria or Prince Albert, were domestic in character, described in *The Times* (permitted advance viewing, and apparently at that stage ignorant of the royals' lack of knowledge of events) as including 'several portraits of the Princess Royal, taken from life by her Majesty . . . in the arms of her nurse, playing and rolling on the carpet with her doll and other toys, amusing herself with the Prince of Wales' and 'portraying other domestic and interesting scenes in the Royal nursery': *The Times* (London), 7 September 1848, p. 5.

[11] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652; 64 ER 293.

[12] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 23; 47 ER 1302 at 1310.

[13] Indeed, the original claim by Prince Albert, later amended, was that the etchings had been stolen from the plaintiff's private apartment: *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 652–7; 64 ER 293 at 293–5.

[14] *Abernethy* v. *Hutchinson* (1825) 3 LJ 209; 47 ER 1313, a case concerning the unauthorised publication of Abernethy's lectures, most likely but not necessarily originating in one of his pupils.

in which Strange was implicated by his knowledge.[15] Such language left the way open in later cases for wrongful obtaining in itself to become the basis of a trust obligation – albeit this took some time, and not all courts in all jurisdictions were ready or able to accept the position. (Even in the United Kingdom it was only finally confirmed at the highest level with the House of Lords decision in *Campbell* v. *MGN Ltd.*[16])

Violation of property right

The Lord Chancellor did not restrict his grounds to breach of trust and confidence, for he referred also to the 'right and property' in the etchings, which the plaintiff was 'entitled to keep wholly for his private use and pleasure', as justifying an injunction against unauthorised publication.[17] Knight Bruce V-C had reached a like conclusion.[18] The language of 'property' is reflective of the times. By the mid-nineteenth century, property was understood to be the starting point of a market economy. Having something to trade was seen as fundamental to participation in its commercial and social institutions and a particularly respected source of wealth was labour and ingenuity which, marshalled to the needs of the market, could become a pathway to prosperity and progress.[19] Enabling a market lay at the heart of many nineteenth-century cases of confidential information. Trade secrets were often labelled 'property'.[20] So too were unpublished texts, including texts of a more personal kind as with the royal family etchings – even if here it was acknowledged that value might be found not

[15] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 23; 47 ER 1302 at 1311.

[16] *Campbell* v. *MGN Ltd* [2004] 2 AC 457. It may be noted that the Law Lords were not always entirely clear that the reasoning was not premised on a very extended idea of the relationship of confidence: see, e.g., Lord Hope at para. 85. In this respect Australian courts have been clearer, positing that surreptitious obtaining is in itself a violation of an obligation of trust and confidence, arising even as between strangers: see *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 at paras. 39–40 (Gleeson CJ), para. 123 (Gummow and Hayne JJ) and para. 223 Callinan J. On the other hand Australian courts may yet find other reasons to consider breach of confidence a limited vehicle for celebrity privacy protection; and the possibility of a tort of privacy was not foreclosed in *Lenah Game Meats*.

[17] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 22; 47 ER 1302 at 1310.

[18] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 697–8; 64 ER 293 at 312–13.

[19] See Brad Sherman and Lionel Bently, *The Making of Modern Intellectual Property Law* (Cambridge: Cambridge University Press, 1999) chap. 9 (although putting fuller development later than the middle of the century).

[20] As, for instance, in the secret recipe case *Morison* v. *Moat* (1851) 9 Hare 241; 68 ER 492 (although Turner V-C noted the basis might equally be breach of contract or trust or confidence).

just in market exchange but in private use, including private circulation among family and friends, as was common at the time.[21] Recognised as 'the produce of mental labours, thoughts and sentiments recorded and preserved by writing' and 'desired by the author to remain not generally known',[22] the right of publication of such texts was reserved to the author on the basis of a property right in the unpublished work, supplementing the various statutory copyrights in published works. 'Common law copyright' has now been abolished by the statutory copyright system,[23] but in 1849 it was well-established. As Lord Cottenham LC said, '[t]he property in an author or composer of any work, whether of literature, art or science, such work being unpublished and kept for his private use or pleasure, cannot be disputed after the many decisions in which that proposition has been affirmed or assumed'.[24] The issue was simply its scope. It was clear that it prevented publication of the etchings after royal permission was refused, as Strange conceded. Nevertheless he contested the right to prevent publication of the descriptive catalogue, arguing this gave information about but did not publish the etchings themselves. The argument failed to persuade either the Vice-Chancellor or the Lord Chancellor who observed that 'a copy or impression of the etchings could only be a means of communicating the knowledge and information of the original'.[25] The conclusion: the choice to exploit publicly the property or else to keep it for 'private use or pleasure' was the author's choice alone.[26]

One common conception about nineteenth-century literary and artistic property is that the romantic idea of the author-genius exerted some

[21] Certainly in the case of Queen Victoria whose attachment to multiplying images was legendary: Winslow Ames, *Prince Albert and Victorian Taste* (London: Chapman & Hall, 1968) pp. 23–4.

[22] The language is Knight Bruce V-C's in *Prince Albert* v. *Strange* 2 De G & SM 652; 64 ER 293 at 311–12. Sherman and Bently suggest that references to 'mental labour' in nineteenth-century cases revealed a lingering pre-industrial natural rights style of reasoning, eventually to be largely superseded by a more overtly utilitarian judicial focus on the value of the product: see above n. 19. But in fact Knight Bruce V-C was quite concerned with the value of the product: see below n. 31.

[23] Copyright Act 1911 (UK), s. 31. See generally Francis E. Skone James, *Copinger on the Law of Copyright* (6th edn, London: Sweet & Maxwell, 1927) pp. 21–2.

[24] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 21; 47 ER 1302 at 1310.

[25] 1 H & TW 1 at 22; 47 ER 1302 at 1310. As Skone James notes herein lies one important point of difference with statutory copyright in unpublished works after the 1911 Act, since by that Act the right of publication given to the author (under s. 1(2)) was restricted to the right to circulate copies of the work to the public: *Copinger*, above n. 23, pp. 33–4.

[26] 1 H & TW 1 at 22; 47 ER 1302 at 1310 (Lord Cottenham LC).

influence over the principles applied.[27] In reality, in these utilitarian times the emphasis was on the value to be found in the work by its audience. As early as 1741 Lord Hardwicke LC in *Pope* v. *Curl*[28] avoided references to the brilliance of Alexander Pope (although Pope himself did not)[29] in concluding his letters could not be made the subject of unauthorised publication by the printer Curl, observing that letters written on 'familiar subjects', 'perhaps never intended to be published', may be of 'more service to mankind', than any that are 'elaborately written and originally intended for the press'.[30] By the time of *Prince Albert* v. *Strange* any residue of eighteenth-century romantic reasoning about authorial genius that might be discerned in earlier cases was actively disclaimed. 'The author of a manuscript, whether he is famous or obscure, low or high' and whether the work is 'interesting or dull, light or heavy, saleable or unsaleable' has 'a right to say of them', Knight Bruce V-C concluded at first instance, adding the law's foundation was 'not . . . referable to any consideration peculiarly literary';[31] a sentiment apparently endorsed in Lord Cottenham LC's words that 'the property in *any* work, whether of literature, art or science, such work being unpublished and kept for his private use or pleasure cannot be disputed' (emphasis added).[32] In part, these statements may have been given in response to a suggestion in the descriptive catalogue that the etchings' superior quality warranted their publication,[33] a suggestion evidently contested by Prince Albert. Yet it was already clear in mid-Victorian England that there were many reasons why a work might be popular – reasons which might have little to do with the superior quality of the work and a great deal to do with the celebrity of the author. When it came to material of a personal kind, Knight Bruce V-C intimated, what was really desired was authenticity – an insight into 'the bent and turn of the mind, the feelings and taste of the artist, especially if

[27] For the romantic idea of the author-genius, which was actively promoted by some Victorian authors, such as Wordsworth, see Peter Jaszi, 'Introduction' in Martha Woodmansee and Peter Jaszi, *The Construction of Authorship: Textual Appropriation in Law and Literature* (Durham: Duke University Press, 1994) p. 1 at pp. 4–6 especially.

[28] *Pope* v. *Curl* (1741) 2 Atk. 342; 26 ER 608.

[29] The story of the case is told in Mark Rose, 'The Author in Court: *Pope* v. *Curll* (1741)' in Woodmansee and Jaszi, *Construction of Authorship*, above n. 27, p. 211.

[30] *Pope* v. *Curl* (1741) 2 Atk. 342 at 343; 26 ER 608 at 608.

[31] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 694–5; 64 ER 293 at 311.

[32] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 21; 47 ER 1302 at 1310.

[33] See *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 653; 64 ER 293 at 294 (recording that the title page of the catalogue referred to the public's interest in admiring and appreciating 'the eminent artistic talent and acquirements of both Her Majesty and her illustrious Consort').

not professional' but rather 'a man on account of whose name alone . . . [the information] would be a matter of general curiosity'.[34]

Passing off

Of course, once it was accepted that insight into a celebrity's 'bent and turn of the mind' and 'feelings and taste' was the public's true desire it was a small step to acknowledge that authenticity may not require authorship, at least in any obvious sense of 'clothing our conceptions in words' (as William Blackstone put it in *Tonson* v. *Collins*).[35] A third claim in *Prince Albert* v. *Strange*, introduced before Lord Cottenham LC, was not based on violation of a property right in the etchings (or even breach of trust), but on a statement in the defendant's catalogue giving the false impression that both the catalogue and the exhibition it purportedly accompanied were authorised, and therefore authentic. In this early age of character merchandising, especially as to royal memorabilia,[36] it was plainly thought a ready market could be found both for the exhibition and for the catalogue, especially if the latter not only gave a list and description of the works but also had inscribed on its title page that:[37]

> Every purchaser of this Catalogue will be presented (by permission) with a facsimile of the autograph of either Her Majesty or of the Prince Consort, engraved from the original, the selection being left to the purchaser.
>
> Price Sixpence

If Knight Bruce V-C had earlier expressed doubts as to the genuineness of the defendant's assumption that permission would be obtained before the exhibition went ahead (voicing a suspicion that the entire rather bizarre

[34] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 694; 64 ER 293 at 311. Certainly this appeared to be *The Times*' perception of the public's interest in the exhibition, commenting in enthusiastic detail on the subject matter of the etchings rather than any perceived expertise exhibited in the artwork (especially in the case of those done by Queen Victoria): see above n. 10.

[35] (1760) 1 Black W 301 at 323; 96 ER 169 at 181.

[36] See 'Victorian Collectibles' and 'Craze for Royal Relics' published by Collector Cafe at http://www.collectorcafe.com/article.asp?article = 650 (noting that the craze 'seems to have developed in the mid-nineteenth century, reflecting a restoration of the British royal family in the public esteem'). For commemorative plates, cups and saucers as a particular category of collectibles in this newly industrial age, see G. Bernard Hughes, *Victorian Pottery and Porcelain* (London: Country Life, 1959) pp. 87, 143 and 149 especially. Dedications 'by permission' were also not uncommon in this period: see, e.g., John Gould, *Birds of Australia* (Part XXVI, London: John Gould, 1847) where the inscription reads 'dedicated by permission to her Majesty'.

[37] See *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 653; 64 ER 293 at 294.

project was a ploy erected around a plan to be 'bought off'), the proceedings continued on the basis of the 'overt acts'.[38] These, Lord Cottenham LC held, were enough to establish a 'falsehood on the public', for 'as permission so to accompany each catalogue sold necessarily implies permission to sell the catalogue itself, the case is complete of an intention to sell under a false representation that the whole transaction is not only with the knowledge but with the approbation of the Plaintiff'.[39] The reference to 'false representation' evokes the emerging action of passing off.[40] In the twenty-first century we have become accustomed to think the practice of character merchandising a recent phenomenon, and with that the extension of laws about false representations to representations of sponsorship or approval.[41] Yet, in this early case, we can already see the beginnings of an understanding that if the purchasing public places value on a celebrity's personal endorsement of goods or services, there may be more than one reason to insist that a claimed endorsement be given.

Admittedly, in *Clark* v. *Freeman*,[42] decided the year before, an eminent royal physician and expert on consumptive complaints could not prevent an apothecary selling a quack medicine promoted as 'Sir J Clarke's consumption pills' – the case later taken as authority for a 'common field of activity' rule which dogged the law of passing off through much of the twentieth century.[43] A merely libellous publication was not thought by Lord Langdale MR, who recalled the dark days of the Star Chamber, to warrant an injunction. Such conduct was, it was said, 'one of the taxes' to

[38] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 688; 64 ER 293 at 308.

[39] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 9; 47 ER 1302 at 1309, continuing that the case was like one of 'manufacturers [who] are, as a matter of course, restrained from selling their goods under similar misrepresentations, tending to impose on the public and to prejudice others'. *The Times* agreed that 'why indeed' should the defendant be exempt from the rule applying to manufacturers: *The Times* (London), 9 February 1849, p. 5.

[40] See William Morison, 'Unfair Competition and Passing Off' (1956) 2 *Sydney Law Review* 50 at 53–5, pointing out that this was a strange action in fraud which, though based in public deception, gave a right to a person complaining of a name falsely used.

[41] See, e.g., *Re American Greetings Corp's Application; sub nom Holly Hobbie Trade Mark* [1984] RPC 349, Lord Bridge at 350, Lord Brightman at 356 referring to what is 'now widely known as "character merchandising"' as having 'become a widespread practice'; and *Pacific Dunlop Ltd* v. *Hogan* (1989) 14 IPR 398 at 429 (Burchett J) (attributing the rise of the practice to television).

[42] (1848) 11 Beav. 112; 50 ER 759.

[43] See Morison, 'Unfair Competition', above n. 40, 60–1. Australian courts were among the first not to follow the authority of *McCulloch* v. *May* (1945) 65 RPC 48, in which the 'common field of activity' rule was stated, based on a narrow reading of *Clark* v. *Freeman*: see *Radio Corporation* v. *Henderson* [1960] NSWR 279. This opened the way for passing off to extend to unauthorised character merchandising at a much earlier stage than in the United Kingdom: see generally *Irvine* v. *Talksport Ltd* [2002] 2 All ER 414 at 421–6 (Laddie J).

which persons of high station become subject 'by the very eminence they have acquired in the world'.[44] However, in seeking the injunction Clark could not show his professional income prejudiced from such statements, which by his own account were unlikely to be believed by the medical professionals who might ask his advice. In the different circumstances of *Prince Albert* v. *Strange*, royal patronage of public events, especially of the arts, was established,[45] and the misrepresentation was directed to the paying public who might be misled by a falsehood that consent had been obtained. Further, the possibility of the plaintiff wishing to give his endorsement in more suitable circumstances was not foreclosed. The Solicitor-General posited that at some later date a royally approved exhibition of the etchings might be permitted, say for charitable purposes, adding 'if that so happened, could it be doubted that a descriptive catalogue . . . would be a very important ingredient of the profit to be derived for such a purpose, or that the property or value would have been materially deteriorated by a premature circulation which had tended to satiate the public interest in the circumstance?'[46] For Lord Cottenham LC, considerations of property – at least in the etchings and perhaps in some broader sense of tradable patronage – made it possible to distinguish *Clark* v. *Freeman* and to bring the case within the boundaries of established authority.

Had there been a need to resolve the issue of passing off in *Prince Albert* v. *Strange*, a more precise account of the property at stake might have been given. It might have been made clearer that this lies, as is now largely accepted, in tradable goodwill, defined as 'the attractive force that brings in custom'.[47] Further, that for celebrities, their ability to provide patronage – to give authority, and through that authenticity, to claims made by traders about their goods or services (including especially those that reveal something of the celebrity's own 'bent and turn of the mind, . . . feelings and taste') – is a form of goodwill.[48] But, perhaps anticipating what would come after the award of an injunction narrowly framed to

[44] (1848) 11 Beav. 112 at 119; 50 ER 759 at 762.

[45] In commenting *The Times* (London), 30 October 1848 p. 6, notes that 'Her Majesty and the Prince are well known as patrons of the arts'. See also Ames, *Prince Albert*, above n. 21, pp. 24–5, although it may be noted that Prince Albert's greatest event of public patronage (the Great Exhibition of 1851) was still to come.

[46] 2 De G & SM 652 at 676–7; 64 ER 293 at 304.

[47] See *Erven Warnink BV* v. *J Townend & Sons (Hull) Ltd* [1979] AC 731 at 741 (Lord Diplock).

[48] It was clear at least in *Radio Corporation* v. *Henderson* [1960] NSWR 279 that a celebrity might trade in the opportunity to 'bestow their name', at 285 (Evatt CJ and Myers J); cf. *Irvine* v. *Talksport* [2002] 2 All ER 414 at 424 (Laddie J), not disapproved on appeal: *Irvine* v. *Talksport Ltd* [2003] 2 All ER 881. Note also the statement of Burchett J in *Pacific Dunlop* v.

prohibit sales *only* of catalogues inscribed *as permitted*, the issue was left there. No doubt the market for unauthorised character merchandising was less developed in Victorian times than now, when authority is no longer considered a particularly reliable guarantee of authenticity. If anything the opposite, as in *Douglas* v. *Hello!* where the unauthorised publication was presented as giving 'real' wedding pictures that the celebrity couple would *not* necessarily wish to have shown.[49] Even so it would seem the desire for royal relics that then existed was such that an audience of sorts could probably be found.[50] Thus, as in modern character merchandising cases where a misrepresentation of endorsement or approval is still an element of passing off, at least in the legal discourse,[51] it was decided a broader basis had to be found in Prince Albert's case for grant of an injunction against the authorised exploitation of material of a private and personal kind – a basis found in common law copyright and breach of trust and confidence.

Invasion of privacy

Privacy was not a cause of action in *Prince Albert* v. *Strange*; nor was it clear what function, if any, privacy should have. Was privacy protection incidental to a property right, as the Solicitor-General maintained;[52] or was privacy, as Strange argued, an interest distinct from property and one not yet recognised in equity or law?[53] In response to the latter argument, Knight Bruce V-C observed that 'there are several offences against

Hogan (1989) 14 IPR 398 that what character merchandising sells is the 'association of some desirable character with the product'.

[49] The cover of the relevant issue of *Hello!* indeed bore the words: 'From New York: The Full Story – Catherine and Michael's Wedding': *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996 at para. 6.

[50] See 'Craze for Royal Relics' above n. 36, noting, e.g., the existence of a market for sales of bloomers with the Queen's monogram, which abated only when it was realised that these were issued to everyone in the royal household 'down to the scullery maid'.

[51] Although Australian courts have certainly been particularly liberal in their readiness to find a misrepresentation established; see, e.g., *Pacific Dunlop Ltd.* v. *Hogan* (1989) 14 IPR 398, passing off (as well as misleading or deceptive conduct under the Trade Practices Act 1974 (Cth)) found on very little evidence of confusion to subsist in a false suggestion of Hogan's agreement to his Crocodile Dundee character being spoofed by a look-alike character in the defendant's advertisements for shoes. The remedy there was limited to damages or account of profits plus a suitable disclaimer; but in other cases, including *Radio Corporation* v. *Henderson* [1960] NSWR 279, a full injunction has been granted.

[52] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 671; 64 ER 293 at 301; reiterated in *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 13; 47 ER 1302 at 1307.

[53] *Ibid.* 2 De G & SM 652 at 680–1; 64 ER 293 at 305; reiterated *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 12; 47 ER 1302 at 1306.

propriety and morals, which, though causing most serious discomfort, pain and affliction to individuals, the law refuses to treat as actionable, unless those offences have occasioned some recognisable damage of a particular kind'.[54] However, the Vice-Chancellor added, 'the principle of protecting property . . . shelters the privacy and seclusion of thoughts and sentiments committed to writing and desired by the author to remain not generally known'.[55] In such cases, the Vice-Chancellor acknowledged, reaping public reward from mental labour may not really be the claimant's object, for 'a man may employ himself in private in a manner very harmless, but which, disclosed to society, may destroy the comfort of his life', revealing as it does an aspect of himself 'of a kind squaring in no sort with his outward habits and worldly position'.[56] Nevertheless, the vindication of privacy by a property right was rationalised under the rubric of property – identifying a sphere of 'private use or private amusement' for the 'various forms and modes of property which peace and cultivation might discover and introduce'.[57] The Lord Chancellor went further, suggesting that where a composition is of a 'private character'[58] and 'kept private',[59] the author has 'a right to the interposition of this Court to prevent any use being made of it' in breach of confidence,[60] adding that where 'privacy is the right invaded' delaying an injunction is equivalent to 'denying it altogether'.[61] The statement reveals some quite interesting thinking. Unlike a property right where the ability to restrain publication was in

[54] Ibid. 2 De G & SM 652 at 689–90; 64 ER 293 at 309, adding however that if a remedy can otherwise be granted the breach of propriety and morals may then be brought into account.

[55] Ibid. 2 De G & SM 652 at 695; 64 ER 293 at 312.

[56] Ibid. 2 De G & SM 652 at 694; 64 ER 293 at 311.

[57] Ibid. 2 De G & SM 652 at 695–6; 64 ER 293 at 311–12.

[58] *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 23; 47 ER 1302 at 1309. Is 'private character' to be taken as more than simply confidential, or non-public: connoting personal intimacy? It is not entirely clear but the *Oxford English Dictionary Online* suggests such a meaning was in use ('privacy' defined to include 'a private matter, a secret; in *pl.* private or personal matters or relations').

[59] The words 'kept private' used in the sense that 'any licence or authority for publication is negatived' (disclosures to 'private friends' not implying 'any such licence or authority') as is the possibility of access by others except by surreptitious or improper means: *Prince Albert* v. *Strange* (1849) 1 H & TW 1 at 23; 47 ER 1302 at 1311.

[60] Ibid. 1 H & TW 1 at 25; 47 ER 1302 at 1311, although going on to state in language more redolent of property that what is meant is that '[the author] is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his own' – suggesting Lord Cottenham may not be entirely sure of his more unqualified pronouncements that the entitlement which breach of confidence recognises does (or should) not depend on whether the privacy claimant would use or enjoy the information.

[61] Ibid. 1 H & TW 1 at 26; 47 ER 1302 at 1312.

this utilitarian age premised on rewarding and encouraging activities the products of which may be found enjoyable or useful by an audience (if only of private friends or even the author alone), when it comes to breach of trust and confidence the choice not to publish 'private' information 'kept private' may be a matter of personal choice which others should be trusted to respect on this account alone.

The reasons for giving accord to personal choice over private matters were not articulated in *Prince Albert* v. *Strange* and may not even have been fully understood in the very middle of the nineteenth century.[62] John Stuart Mill's influential argument in *On Liberty* that individual flourishing in an atmosphere of freedom is good not only for the individual but for society, was still to come. It was only in 1859 that Mill was to elaborate the idea that:

> [T]here is a sphere of action in which society, as distinct from the individual, has, if any, only an indirect interest; comprehending all that portion of a person's life and conduct which affects only himself . . . [by which] I mean directly, and in the first instance; . . . [and t]he only freedom which deserves the name, is that of pursuing our own good in our own way, so long as we do not attempt to deprive others of theirs, or impede their efforts to obtain it.[63]

Nevertheless the germ of Mill's thinking was to be found in writings of David Hume and Adam Smith who held that a civil society could only benefit from a high level of respect for individual freedom and control.[64] The early English utilitarians who employed the greatest happiness of the greatest number as the measuring stick of value also argued that happiness for each person is a matter of individual choice.[65] And Mill himself referred to a 'Greek idea of self-development . . . [that i]n proportion to

[62] Certainly *The Times* (the major daily newspaper of the day) in commenting on the case initially offered little further explanation of why Prince Albert and his consort should be protected from 'intrusive vulgarity', in later commentary on Lord Cottenham's judgment referring somewhat more firmly to a 'public's sympathy' with the Royals' feelings that they 'can no longer endure living in a glass house': see above nn. 39 and 45.

[63] 'On Liberty', in John Stuart Mill, *Utilitarianism, On Liberty, Essay on Bentham*, ed. and intro. Mary Warnock (London: Collins, 1962) pp. 126–250 at pp. 137–8.

[64] Indeed Hume and Smith doubted that individual welfare could be promoted otherwise than by each person assuming, as 'befits the narrowness of his comprehension', care of 'his own happiness, or that of his family, his friends' (Smith's words in *Theory of Moral Sentiments*, 1759, VI, ii.3.6); see Jerry Muller, *Adam Smith in His Time and Ours: Designing the Decent Society* (Princeton: Princeton University Press, 1995) chap. 3. Mill himself doubted whether the care of family and friends should even be assumed; see especially 'On Liberty', above n. 63, pp. 205–25.

[65] Mill criticised Bentham for thinking of 'all the deeper feelings of human nature' as 'idiosyncrasies of taste, with which neither the moralist nor the legislator has any concern',

the development of his individuality, each person becomes more valuable to himself, and is therefore capable of becoming more valuable to others'.[66] With such a rich potential base of utilitarian support for privacy as a species of liberty, English courts did not have to embrace the theories of continental European philosophers which treated privacy as an integral part of human dignity and dignity as an immutable end of human existence.[67] Acknowledging privacy as a legitimate matter of individual choice in *Prince Albert* v. *Strange* did not preclude acknowledgment of other legitimate choices that might be made about material of a private personal kind. Even within privacy a choice of private use and enjoyment or simply no use at all could now be imagined. The possibility of the author-subject choosing free public expression, the choice exercised by Mill in writing his *Autobiography* as a means of 'stopping the mouths of enemies hereafter', who whispered scandalous things about his relationship with Harriet Taylor,[68] might also be contemplated. So too could commercial exploitation of the exchange value of any property that might be identified, anticipated in discussions in Prince Albert's case about the prospect of an authorised exhibition. Since privacy was an aspect of liberty whose value was defined in utilitarian terms, grounded according to Mill 'on the permanent interests of a man as a progressive being',[69] recognising the value of privacy did not prevent recognition of other freedoms as important as well. Further, Mill could easily accept that the ability to exercise all these freedoms in a forward looking way and plan

maintaining that there are higher pleasures that are of more enduring happiness than lower pleasures, which those who have experienced both could appreciate: 'Essay on Bentham' in Mill, *Utilitarianism*, above n. 63, pp. 78–125 at p. 101; 'Utilitarianism' in Mill, *Utilitarianism,* ibid. pp. 251–321 at pp. 259–62. Nevertheless in accord with his liberal views, Mill held that it is for the individual to make the ultimate judgment in matters that concern only themselves; and in this respect he was more like Bentham than he cared to admit.

66 'On Liberty' in Mill, *Utilitarianism*, above n. 63, p. 191.

67 Especially Immanuel Kant, 'Groundwork of the Metaphysics of Morals' in Immanuel Kant, *The Moral Law: Kant's Groundwork of the Metaphysic of Morals*, translated and analysed by H. J. Paton (London: Hutchinson University Library, 1948) pp. 90–1, whose precept that persons should be treated as ends in themselves and not means to ends of others was to become the basis of a 'dignitary' idea of privacy in continental Europe and to a lesser extent, under the influence of Warren and Brandeis, the United States: see James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151. But as Mill pointed out, whether Kant's dignitary ideas were truly non-utilitarian, or rather represented his (very extreme) idea of what made for a happier society, is another question: 'Utilitarianism' in Mill, *Utilitarianism*, above n. 63, p. 308.

68 See Jack Stillinger, 'Introduction' in John Stuart Mill, *Autobiography* (London: Oxford University Press, 1971), p. vii.

69 'On Liberty' in Mill, *Utilitarianism*, above n. 63, p. 136.

'beyond the passing moment', capturing value over time, depended on a measure of trust that others would 'join in making safe for us the very groundwork of our existence'.[70] Indeed such ideas were – and continue to be – intricately connected with the development of the equitable action for breach of confidence as a doctrine essentially about freedom (and with that security) of choice.

How little has changed

Table 10.1. *Instances of 'privacy' and 'private' in judgments* [71]

	'privacy'	'private'
Prince Albert v. *Strange* (1849), Cottenham LJ	1	10
Douglas v. *Hello!* (2000), Sedley LJ	50	10
Hosking v. *Runting* (2004), Gault P & Blanchard J	259	102
Campbell v. *MGN* (2004), Lord Hope	26	42
Von Hannover v. *Germany* (2004), the court	32	84

Privacy is more greatly emphasised (and property less) in the recent celebrity privacy cases compared with *Prince Albert* v. *Strange*. As Table 10.1 shows, there was but one reference to 'privacy' and ten to 'private' in the judgment of Lord Cottenham LC, whereas a comparable appellate

[70] Mill is justly famous for his utilitarian arguments for freedom of speech, conduct and property but his argument that 'security, to everyone's feelings the most vital of interests' is also of utilitarian import is equally powerful, and allows us to recognise that the ability to trust in the conduct even of strangers is the basis of a modern liberal welfare society: see 'Utilitarianism' in Mill, *Utilitarianism*, above n. 63, pp. 309–10.

[71] Recorded simply are instances of 'privacy' and 'private' as reported or used in each of the judgments surveyed. To the extent judges simply report what others have said without lending their support, the tallying process may overstate the value accorded by the particular judges, but nevertheless shows something of the value others place on privacy. Undoubtedly some of the increased referencing to privacy/private in English judgments is due to the United Kingdom's implementation of the European Convention on Human Rights with its Article 8 right of 'private life', but New Zealand has no right of privacy in its Bill of Rights and even Australia – which has no Bill of Rights – has seen increased use of privacy language in modern breach of confidence cases: see, e.g., the judgment of Gleeson CJ in *Australian Broadcasting Corporation* v. *Lenah Game Meats* (2001) 208 CLR 199 (15 references to 'privacy', 32 to 'private').

judgment in a modern case can easily multiply such references many times.[72] Thus the conclusion might be drawn that privacy is now a more significant social value than before – or at least that privacy was an emerging value in the Victorian age, whereas its importance is now clearly established.

Whether the current emphasis on privacy supports a conclusion that a shift has occurred towards a dignitary conception, in which privacy is purely and simply a right to be 'let alone', a right of 'inviolate personality', is another matter. In general little support can be found in the cases. Rather, the new talk of privacy appears to reflect a judicial consensus that, as Mill claimed, '[a]mong the works of man which human life is rightly employed in perfecting and beautifying, the first in importance surely is man himself'.[73] Indeed in *Von Hannover* v. *Germany* it was simply stated that the European Convention's right of private life was 'primarily intended to ensure the development of each individual in his relations with other human beings'[74] – suggesting that dignity is not an immutable end of human existence (although it may be a component of flourishing).[75]

Equally, while it is now commonly accepted that 'stars are made for profit' and 'different star images' are presented to the world, from which 'the audience selects . . . the meaning and feelings, the variations, inflections and contradictions, that work for them',[76] the utilitarian logic of treating celebrity stories as warranting protection has not escaped the

[72] By contrast there are no explicit references to 'property' in private information in the above judgments, including the interlocutory judgment of Sedley LJ in *Douglas* v. *Hello!* [2001] QB 967, which refers to the celebrities' privacy as 'sold': at paras. 140–1. In its subsequent decision the Court of Appeal went further in suggesting that the language of property is inappropriate: Lord Phillips MR for the court, [2006] QB 125 at para. 119ff. The conclusion, resting on a rather narrowly confined idea of what constitutes a 'property' right (treating assignability as the *sine qua non* and an option not available to 'owners' of confidential information), may be too strong: see further Megan Richardson, 'Owning Secrets: "Property" in Confidential Information?' in Andrew Robertson (ed.), *The Law of Obligations: Connections and Boundaries* (London: UCL Press, 2004) chap. 9.

[73] 'On Liberty' in Mill, *Utilitarianism*, above n. 63, p. 188.

[74] (2005) 40 EHRR 1 at para. 50.

[75] Similarly, in the privacy tort case *Hosking* v. *Runting* [2005] 1 NZLR 1 dignitary references are interspersed with references to personal flourishing, leading one of us to conclude that a modicum of dignity may be coming to be treated as a component of flourishing and therefore utility: see Richardson, 'Privacy and Precedent' above n. 4, 93. The closest the cases reviewed have come to enouncing a dignitary conception is Lord Sedley's reference to privacy as 'a fundamental value of personal autonomy' in his interlocutory judgment in *Douglas* v. *Hello!* [2001] QB 967 at para. 136 – language avoided by Lindsay J in his judgment, who spoke of confidentiality as a matter of 'control': *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996 at para. 216. In their most recent judgment in the case, the Court of Appeal appeared to support Lindsay J's position in this respect: [2006] QB 125 at para. 118.

[76] Richard Dyer, *Heavenly Bodies: Film Stars and Society* (London: MacMillan, 1987) p. 5.

courts. Thus in *Douglas* v. *Hello!* the celebrities were held entitled to control the way their wedding was portrayed to their public, their right to 'profit from information about themselves' acknowledged.[77] The information shared some characteristics of copyright works, its story-telling quality lying in the myth of the perfect wedding between the perfect couple told to an audience that is at some level aware of the myth.[78] But the more obvious analogy is to trade secrets is in line with references to 'profit to be derived' and 'value . . . materially deteriorated by a premature circulation' in *Prince Albert* v. *Strange*.[79]

Finally, courts working in the tradition of *Prince Albert* v. *Strange* have found it relatively easy to accept that a celebrity may choose to reveal selectively certain personal information, including for profit, yet maintain the privacy of the rest,[80] giving little credence to the idea that privacy cannot be 'wrapped up and sold': the penalty for doing so being privacy obliteration.[81] Celebrities may find themselves subject to certain trust obligations, as Campbell found to her cost in publicly lying about her drug addiction,[82] but courts have stopped short of treating self-publicity as engendering an automatic obligation of utter transparency.[83] Even the language of 'reasonable expectation' of privacy, which features in some

[77] See the Court of Appeal [2006] QB 125 at paras. 113–19ff. and further above n. 72.

[78] Such stories fit a broad idea of literature as 'an organ of myth-making, a part of man's dream of self-definition': see Rene Wellek, 'The Attack on Literature' in Rene Wellek (ed.), *The Attack on Literature and Other Essays* (Chapel Hill: University of North Carolina Press, 1982) p. 3 at p. 10 (referring to Northrop Frye, *Anatomy of Criticism* (Princeton: Princeton University Press, 1957)). Wellek rightly adds they may not be very *good* literature, at p. 17.

[79] 2 De G & SM 652 at 676–7; 64 ER 293 and also (for an analogy drawn to passing off as between 'manufacturers') above n. 39.

[80] See the Court of Appeal in *Douglas* v. *Hello!* [2006] QB 125 at para. 118 where this was stated – although the court appeared later to doubt that significant damages could be obtained for breach after commercialisation, confirming Lindsay J's modest award for 'mental distress' to Douglas and Zeta-Jones and rejecting their argument for a notional licence fee after exclusive rights had been sold to *OK!*: at para. 237ff. and further para. 107 (if anything suggesting there may be reason to reduce damages for mental distress based on the earlier authorisation of filming and publication by *OK!*). The reasoning on remedies may be questioned and no doubt will be the subject of further comment.

[81] Per Jane M. Gaines, *Contested Culture: The Image, the Voice, and the Law* (Chapel Hill: University of North Carolina Press, 1991) p. 186. Cf. the suggestion by Warren and Brandeis, 'The Right to Privacy' above n. 8, at 214–16 that public figures abdicate privacy (in Mill's terms an unacceptable slavery contract: 'On Liberty' in Mill, *Utilitarianism*, above n. 63, p. 236).

[82] *Campbell* v. *MGN Ltd* [2004] 2 AC 457. Query how far such reasoning may be taken.

[83] *Douglas* v. *Hello!* gives a partial exception in the refusal of an interlocutory injunction against publication of the unauthorised wedding pictures on the ground that the claimants' privacy had been 'sold': see above n. 72 (although limiting the qualification to other wedding pictures). Lindsay J in the final proceedings would have allowed the injunction: see *Douglas* v. *Hello! Ltd* [2003] 3 All ER 996 at para. 278; as would the Court of Appeal in

of the recent cases, has not been taken to allow those curious to know to override a privacy subject's choice to maintain privacy if the choice is one that might equally have been made in the privacy subject's place.[84] The conclusion is one that Mill, who hated the 'despotism of custom', would have approved.[85]

On the other hand, more to the foreground now is the role played by the not entirely disinterested agents of public 'exposure' of private, personal celebrity information: the modern self-styled arbiters of custom. Now it is publicly acknowledged by those well-accustomed to its inner workings that 'Fleet Street has always had a two-way relationship with the celebrities. One day you are cock of the walk and the next day you are a feather duster.'[86] However, already by the time of *Prince Albert* v. *Strange* some of the basic features of the modern British media at work could be observed: the itinerant disaffected journalist (the forebear of the modern paparazzi), the profit-motivated publisher, a burgeoning public avid for news – as well as the technologies that permitted not only mass speed printing but also mass distribution of its products.[87] When newspapers were widely available, cheap to read, even cheaper if their contents could be shared in 'the new urban conditions', and popular in reliance on 'habitual tastes and markets' of an increasingly literate public, it is not surprising that they were gathering a substantial following.[88] They commented on

its most recent judgment in the case, especially with the benefit of the decisions that came after in the *Naomi Campbell* and *Von Hannover* cases: [2006] QB 125 at para. 253 ff.

[84] See *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at paras. 94–5 (Lord Hope); *Douglas* v. *Hello!* [2006] QB 125 at para. 107. Gleeson CJ was less clear as to whose judgment should be applied in *ABC* v. *Lenah Game Meats* (and was the first to suggest that a standard of 'highly offensive to a reasonable person' should be adopted, borrowing from US privacy tort cases, and might be part of the test of confidentiality in a breach of confidence/privacy case): (2001) 208 CLR 199 at paras. 39–42.

[85] 'On Liberty' in Mill, *Utilitarianism*, above n. 63, p. 200.

[86] Statement of well-known former Fleet Street tabloid editor Piers Morgan quoted in *Fraser-Woodward Ltd* v. *British Broadcasting Corporation* [2005] EMLR 22 at para. 16 (Mann J).

[87] Steam printing of *The Times* began in 1819, according to Raymond Williams, and this combined with access to a railway network gave established newspapers the possibility of reaching a wider readership (the same technologies facilitating the introduction and spread of alternative publications aimed at new markets): 'The Press and Popular Culture: An Historical Perspective' in George Boyce, James Curran and Pauline Wingate (eds.), *Newspaper History from the Seventeenth Century to the Present Day* (London: Constable, 1978) chap. 2.

[88] See generally Williams, 'The Press and Popular Culture', above n. 87 and further Ivon Asquith, 'The Structure, Ownership and Control of the Press, 1780–1855' in Boyce, Curran and Wingate, *Newspaper History*, ibid. ch 5.

everything including the minutiae of cases before the courts, and on virtually every occasion where an opinion might be given it was expressed; nor was this inevitably favourable to those considered celebrities, especially if the celebrity in question was not an irrevocable part of the establishment – at risk particularly foreigners and anyone whose opinions or beliefs were different from the mainstream.[89] Then, as now, there was also the feverish excitement of the story unfolding from day to day, the future never able to be foretold by an audience hooked on the drip-feed of serialisation through the writings of Charles Dickens and other relaters of fictional yet lifelike stories,[90] with the opportunity for a judgmental response ever-present. A. N. Wilson observes that 'one of the strangest legacies left to the world by the Victorians is the popular press . . . fuelled by sensationalism and moralism', its treatment of information turned into a business enterprise applying a broad Victorian ethos of 'money-making'.[91] The sheer entrepreneurship of the enterprise could be admired – and some of those involved took great personal risks in their efforts to break new ground in the collection and reporting of material.[92] For a while it might have perhaps been imagined that freedom of thought and discussion were

[89] Even figures such as Prince Albert, a German of highbrow taste, were not immune from the perils of changing public opinion: see Reginald Pound, *Albert: A Biography of the Prince Consort* (London: Michael Joseph, 1973) p. 184 and *passim*. (Certainly support for his claim in *The Times* firmed after his success before Lord Cottenham LC: see above n. 62.) Query whether women formed another 'at risk' category: some have observed that modern female stars are particularly vulnerable to critical public opinion: see Richard Dyer, 'Stars as Specific Images', in Dyer (ed.), *Stars*, above n. 76, and this may explain the targeting of Catharine Zeta-Jones and Naomi Campbell for particular media criticism as their cases went to court.

[90] Including George Reynolds (editor of the popular Sunday newspaper *Reynolds's News*), 'who for a number of years outsold even Dickens with his serialised sensational fiction, centred on aristocratic scandals': Williams, 'The Press and Popular Culture', above n. 87, p. 49.

[91] A. N. Wilson, *The Victorians* (London: Arrow Books, 2003) pp. 461–3. Wilson is referring here particularly to the tabloid press that emerged in the second half of the nineteenth century after abolition of stamp duties. But as Williams and others have pointed out, there were ways around the stamp duties and a popular Sunday press could be found earlier in the century: Williams, 'The Press and Popular Culture', above n. 87, pp. 48–50; Asquith, 'Structure, Ownership and Control', above n. 88, 106–7 and Virginia Berridge, 'Popular Sunday Papers and Mid Victorian Society' in Boyce, Curran and Wingate, *Newspaper History*, above n. 87, chap. 13.

[92] Including Judge and Strange from *Prince Albert* v. *Strange*, both of whom became exposed to bankruptcy as a result of the case (even though damages were not claimed and costs were waived or paid by others, a far cry from the situation with modern celebrity privacy cases where costs awards may be even more financially significant than damages): see letters to *The Times* (London), 11 August 1849 (J. T. Judge) and 17 January 1851 ('Justitia').

necessarily promoted by freedom of the press, as contended by Strange in *Prince Albert* v. *Strange*.[93] But even Victorian liberals ultimately had difficulty justifying the press's more muckraking activities in terms of free speech. If anything these could be viewed as efforts at controlling meaning not facilitating greater public understanding, the utilitarian justification for free speech put forward by Mill.[94] And in this, Mill concluded, they were largely successful – referring to:

> . . . [the] mass, that is to say, collective mediocrity . . . [which] do not now take their opinions from dignitaries in Church or State, from ostensible leaders, or from books . . . Their thinking is done for them by men much like themselves, addressing them or speaking in their name, on the spur of the moment, through the newspapers.[95]

However, these concerns were not to be expressed for a decade to come; and it took until after the end of the following century for courts finally to address the problematic question of the public interest in knowing information that is neither political nor especially literary or artistic, but is simply, as Knight Bruce V-C said in *Prince Albert* v. *Strange*, a matter of 'general curiosity'.[96]

By that time, of course, the equitable obligation was already being framed as a filter for acts of 'falsehood or duplicity [as well as] unfair or ungenerous use of advantage' in obtaining and/or using private personal information, being acts which according to Mill 'require a totally different treatment'[97] – and modern courts continue to abide by the dictum in their assessments of whether a breach of confidence has occurred for which a remedy should be given.[98] If anything the language of trust has entered the vernacular of privacy itself – shown by the European Court's emphasis in

[93] *Prince Albert* v. *Strange* (1849) 2 De G & SM 652 at 667; 64 ER 293 at 300 (the argument did not succeed of course).

[94] 'On Liberty' in Mill, *Utilitarianism*, above n. 63, pp. 141–83.

[95] Ibid. 195.

[96] See *Campbell* v. *MGN Ltd* [2004] 2 AC 457 at para. 117 (Lord Hope) (freedom of speech less convincing where 'there are no political or democratic values at stake' and 'no pressing social need' for publication) and *Von Hannover* v. *Germany* (2005) 40 EHRR 1 at paras. 60–6 (if the 'sole purpose [of publication] was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, [this] cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public' and 'in these circumstances freedom of expression calls for a narrow interpretation').

[97] 'On Liberty' in Mill, *Utilitarianism*, above n. 63, p. 209.

[98] See Lindsay J in *Douglas* v. *Hello!* (emphasising the surreptitious and deceitful character of the paparazzi's obtaining of unauthorised wedding photographs, and the defendants' knowledge/notice of this as 'tainting' their conscience and undermining their arguments that the public interest lay with publication): [2003] 3 All ER 996 at para. 198 and paras.

the *Von Hannover* case on the climate of 'continual harassment' suffered by celebrities at the hands of the tabloid press as supporting a claim under Article 8 of the European Convention.[99] It remains to be seen whether trust will become less a part of our confidentiality doctrine in the foreseeable future, as privacy comes more to the fore.

204–5; the Court of Appeal seemed to think that consent to filming by *OK!* reduced the 'offensiveness' of *Hello!*'s action but accepted that 'the intrusion into the private domain is, of itself, objectionable': [2006] QB 125 at para. 107. In *Campbell* v. *MGN Ltd* Lord Hope observed that '[t]he message that [the Mirror's publication] conveyed was that somebody, somewhere, was following [Campbell], was well aware of what was going on and was prepared to disclose the facts to the media'; a factor pertinent to 'confidentiality' and 'an additional element in the publication' that was 'more than enough to outweigh the right to freedom of expression which the defendants are asserting in this case': [2004] 2 AC 457 at paras. 98 and 124; cf. also para. 155 (Baroness Hale).

[99] [2004] EMLR 21 at paras. 59 and 68 (noting that although the present application concerned only publications, 'the context in which these photos were taken without the applicant's knowledge or consent and the harassment endured by many public figures in their daily lives cannot be fully disregarded').

BIBLIOGRAPHY

Aikman, Colin C., 'Recent Constitutional Changes in the South-West Pacific' in *1968 New Zealand Official Yearbook* (Wellington: Government Printer, 1968)

Alderman, Ellen and Kennedy, Caroline, *The Right to Privacy* (New York: Alfred A. Knopf, 1995)

Allen, Anita L. and Mack, Erin, 'How Privacy Got Its Gender' (1990) 10 *Northern Illinois University Law Review* 441

Ames, Winslow, *Prince Albert and Victorian Taste* (London: Chapman & Hall, 1968)

Amestoy, Jeffrey L., 'Uncommon Humanity: Reflections on Judging in a Post-Human Era' (2003) 78 *New York University Law Review* 1581

Anderson, David A., 'The Failure of American Privacy Law' in Basil S. Markesinis (ed.), *Protecting Privacy* (Oxford: Oxford University Press, 1999)

Article 29 Working Party, *Working Document on Data Protection Issues related to RFID Technology*, 10107/05/EN, WP 105, 19 January 2005

Working Document on Data Protection Issues related to Intellectual Property Rights, WP 104, 18 January 2005

Working Document on Transfers of Personal Data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, MARKT/11639/02/EN, WP 74, 3 June 2003

Opinion 2/2002 on the use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of Ipv6, 10750/02/EN/final, WP 58, 30 May 2002

Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Websites, 5035/01/EN/Final, WP 56, 30 May 2002

Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000, 5095/00/EN, WP 40, 26 January 2001

Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, DG MARKT 5093/98, WP 17, 23 February 1999

Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), XV D/5032/98, WP 11, 16 June 1998

Recommendation 3/97: Anonymity on the Internet, DG MARKT D/5022/97, WP 6, 3 December 1997

Asia-Pacific Economic Cooperation, *Report of the APEC Electronic Commerce Steering Group 11th Meeting*, 2005/SOM I, 24–25 February 2005

APEC Ministers Endorse the APEC Privacy Framework, Media Release, Santiago, Chile, 20 November 2004, available from http://www.apec.org/apec/news_media/2004_media_releases.html

Asia-Pacific Privacy Charter Council, *Submission to the APEC Electronic Commerce Steering Group Privacy Sub-Group* (31 May 2004), available at http://www.bakercyberlawcentre.org/appcc/APEC_APPCCsub.htm

Australia, Copyright Convergence Group, *Highways to Change – Copyright in the New Communications Environment* (Canberra: AGPS, 1994)

Australia, Department of Communications, Information Technology and the Arts, *A Guide to Digital Rights Management* (Canberra: DCITA, 2002)

Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Inquiry into Technological Protection Measures (TPM) Exceptions* (Canberra: House of Representatives, 1 March 2006)

Australia, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (March 2005)

Australia, Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (Canberra: Senate Printing Unit, June 2005)

Australian Law Reform Commission, *Privacy*, Report No. 22 (Canberra: AGPS, 1983)

Australian Privacy Foundation, *Submission to Senate Legal and Constitutional Inquiry into Privacy Act 1988* (March 2005)

Barendt, Eric, *Freedom of Speech* (2nd edn, Oxford: Oxford University Press, 2005)

'Privacy and the Press' in Barendt, Eric M. (ed.), *Yearbook of Media and Entertainment Law 1995* (Oxford: Clarendon Press, 1995)

Becker, Eberhard, Buhse, Willms, Günnewig, Dirk and Rump, Niels (eds.), *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (Lecture Notes in Computer Science Vol. 2770) (Berlin: Springer, 2003)

Belgian Privacy Commission, *Opinion on the Protection of the Privacy of Minors on the Internet*, Avis no. 38/2002, 16 September 2002

Bennett, Colin J. and Raab, Charles D., *The Governance of Privacy: Policy Instruments in Global Perspective* (London: Ashgate, 2003)

Bernstein, Gaia, 'Information Technologies and Identity' [2005] 1 *Computer Law Review International (formerly Computer und Recht International)* 1

Blasi, Vincent, 'Learned Hand and the Self-Government Theory of the First Amendment: *Masses Publishing Co.* v. *Patten*' (1990) 61 *University of Colorado Law Review* 1

Bloustein, Edward J., 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962

Bok, Sissela, *Secrets: On the Ethics of Concealment and Revelation* (New York: Pantheon Books, 1982)

Boulanger, Marie-Hélène and de Terwangne, Cécile, 'Internet et le respect de la vie privée' in Montero, Etienne (ed.), *L'internet face au droit*, Cahier du CRID no. 12 (Namur: Story-Scientia, 1997)

Bowrey, Kathy, *Law and Internet Cultures* (Cambridge: Cambridge University Press, 2005)

Boyce, George, Curran, James and Wingate, Pauline (eds.), *Newspaper History from the Seventeenth Century to the Present Day* (London: Constable, 1978)

Braithwaite, John and Drahos, Peter, *Global Business Regulation* (Cambridge: Cambridge University Press, 2000)

Brennan, William J., Jr, 'Reason, Passion, and "The Progress of the Law"' (1988) 10 *Cardozo Law Review* 3

'The Constitution of the United States: Contemporary Ratification' (1985) 27 *South Texas Law Review* 433

'The Supreme Court and the Meiklejohn Interpretation of the First Amendment' (1965) 79 *Harvard Law Review* 1

Burrows, John and Cheer, Ursula, *Media Law in New Zealand* (5th edn, South Melbourne: Oxford University Press, 2005)

Campbell, Emily, 'Mandatory AIDS Testing and Privacy: A Psycholegal Perspective' (1990) 66 *North Dakota Law Review* 449

Cardozo, Benjamin N., *The Nature of the Judicial Process* (New Haven: Yale University Press, 1921)

Carter, David and Palmer, Mathew (eds.), *Roles and Perspectives in the Law: Essays in Honour of Sir Ivor Richardson* (Wellington: Victoria University Press, 2002)

Catlett, Jason, *Open Letter 9/13 to P3P Developers*, 13 September 1999, available at http://www.junkbusters.com/standards.html

Clarke, Roger, 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000), available at http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html

'The Digital Persona and its Application to Data Surveillance' (1994) 10 (2) *The Information Society*, available at http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html

Cohen, Julie E., 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 *Stanford Law Review* 1373

'DRM and Privacy' (2003) 18 *Berkeley Technology Law Journal* 575

'Normal Discipline in the Age of Crisis' (Draft, 4 August 2004), see http://www.ssrn.com

Cohen-Almagor, Raphael, *Speech, Media and Ethics: The Limits of Free Expression* (Basingstoke, UK: Palgrave, 2001)

Coleman, Jules and Shapiro, Scott (eds.), *The Oxford Handbook of Jurisprudence & Philosophy of Law* (Oxford: Oxford University Press, 2002)

Colvin, Madeleine (ed.), *Developing Key Privacy Rights* (Oxford: Hart, 2002)

Council of Europe, *Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the Purpose of Prevention, Investigation, Detection and Prosecution of Crime and Criminal Offences including Terrorism*, 8958/04, CRIMORG 36, TELECOM 82, 28 April 2004

Council of Europe, Committee of Ministers, *Guidelines for the Protection of Individuals with regard to the Collection and Processing of Personal Data on Information Highways*, Recommendation no. R (99) 5, 23 February 1999

Damich, Edward J., 'The Right of Personality: A Common-Law Basis for the Protection of the Moral Rights of Authors' (1988) 23 *Georgia Law Review* 1

DeCew, Judith Wagner, *In Pursuit of Privacy* (Ithaca, New York: Cornell University Press, 1997)

Delbar, Catherine, Mormont, Marinette and Schots, Marie, (European Industrial Relations Observatory Online), *Comparative Report on New Technology and Respect for Privacy at the Workplace*, TN0307101S, 12 August 2003

Dent, Chris and Kenyon, Andrew T., 'Defamation Law's Chilling Effect: A Comparative Content Analysis of Australian and US Newspapers' (2004) 9 *Media & Arts Law Review* 89

Dewey, John, *Democracy and Education* (New York: Macmillan, 1961)

Dhont, Jan and Perez-Asinari, María Verónica, 'New Physics and the Law: A Comparative Approach to the EU and US Privacy and Data Protection Requirement – Looking for "Adequate Protection"' in Mensbrugghe, F. van der (ed.), *L'utilisation de la méthode comparative en droit européen –Usage of Comparative Methodology in European Law* (Belgium: Presses Universitaires de Namur, 2003)

Dhont, Jan, Pérez-Asinari, María Verónica and Poullet, Yves (with the assistance of Reidenberg, Joel R. and Bygrave, Lee A.), *Safe Harbour Implementation Study* (Namur: CRID, 2004)

Dinant, J. Marc, 'Law and Technology Convergence in the Data Protection Field' in Walden, Ian and Hörnle, Julia (eds.), *E-Commerce Law and Practice in Europe* (Cambridge: Woodhead, 2002)

'Le visiteur visité – Quand les éditeurs de logiciel internet passent subrepticement à travers les mailles du filet juridique' (Winter 2001) 6:2 *Lex Electronica*, available from http://www.lex-electronica.org

Dobbs, Dan B., *The Law of Torts* (St Paul, Minn.: West, 2000)

Dworkin, Ronald, *A Matter of Principle* (Cambridge, Mass.: Harvard University Press, 1985)

Dyer, Richard, *Heavenly Bodies: Film Stars and Society* (London: MacMillan, 1987)

Eberle, Edward J., 'Human Dignity, Privacy, and Personality in German and American Constitutional Law' [1997] *Utah Law Review* 963

Ely, John Hart, *Democracy and Distrust: A Theory of Judicial Review* (Cambridge, Mass.: Harvard University Press, 1980)

'The Wages of Crying Wolf: A Comment on *Roe* v. Wade' (1973) 82 *Yale Law Journal* 920

Emerson, Thomas I., 'The Right of Privacy and Freedom of the Press' (1979) 14 *Harvard Civil Rights–Civil Liberties Law Review* 329

'Toward a General Theory of the First Amendment' (1963) 72 *Yale Law Journal* 877

European Commission, *Seventh Report on the Situation regarding the Protection of Individuals with regard to the Processing of Personal Data and Privacy in the European Union and in Third Countries* (Luxembourg: Office for Official Publications of the European Communities, 2004)

Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Unsolicited Commercial Communications or 'Spam', COM(2004) 28, 22 January 2004

Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data (30 October 2002)

Digital Rights: Background, Systems, Assessment, Commission Staff Working Paper, SEC(2002) 197, 14 February 2002

Copyright and Related Rights in the Information Society: Green Paper from the European Commission to the European Council, COM/95/0382 final, 19 July 1995

European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system)*, 2001/2098(INI)

Faulks, Sebastian, *The Fatal Englishman* (London: Random House, 1996)

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

Ficsor, Mihaly, *The Law of Copyright and the Internet: The 1996 WIPO Copyright Treaties, their Interpretation and Implementation* (Oxford: Oxford University Press, 2002)

Fineman, Martha A., 'Intimacy Outside of the Natural Family' (1991) 23 *Connecticut Law Review* 955

Fish, Stanley, *There's No Such Thing as Free Speech* (Oxford: Oxford University Press, 1994)

Flew, Terry, *New Media: An Introduction* (2nd edn, South Melbourne: Oxford University Press, 2005)

Ford, Peter, 'Implementing the Data Protection Directive – An Outside Perspective' (2003) 9 *Privacy Law & Policy Reporter* 141

Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, transl. Sheridan, Alan (Harmondsworth: Penguin, 1979)

Frame, Alex, 'Lawyers and the Making of Constitutions: Making Constitutions in the South Pacific' in Carter, David and Palmer, Mathew (eds.), *Roles and Perspectives in the Law: Essays in Honour of Sir Ivor Richardson* (Wellington: Victoria University Press, 2002)

Franzen, Jonathan, *How to be Alone* (London: Harper Collins, 2002)

Freund, Paul A., *On Law and Justice* (Cambridge, Mass.: Belknap Press of Harvard University Press, 1968)

Friedman, David D., Landes, William M. and Posner, Richard A., 'Some Economics of Trade Secret Law' (1991) 5 *Journal of Economic Perspectives* 61

Frye, Northrop, *Anatomy of Criticism* (Princeton: Princeton University Press, 1957)

Gavison, Ruth, 'Too Early for a Requiem: Warren and Brandeis were Right on Privacy vs Free Speech' (1992) 43 *South Carolina Law Review* 437

Geller, Paul Edward, 'Toward an Overriding Norm in Copyright: Sign Wealth' (1994) 159 *Revue Internationale du Droit d'Auteur (RIDA)* 3

Georges, Marie, 'Relevons les défis de la protection des données à caractère personnel: l'Internet et la CNIL' in Lemoire, P. (ed.), *Commerce électronique-Marketing et vie privée* (Paris: LaSer, 1999)

Ginsburg, Jane C., 'How Copyright Got a Bad Name for Itself' (2002) 26 *Columbia Journal of Law and the Arts* 61

'Copyright or 'Infograb': Comment on General Report on Limitations Found Outside Copyright' in Baulch, Libby, Green, Michael and Wybum, Mary (eds.), *The Boundaries of Copyright, its Proper Limitations and Exceptions*, (Sydney: ALAI Study Days, Australian Copyright Council, 1999)

Ginsburg, Jane C. and Besek, June M. (eds.), *Adjuncts and Alternatives to Copyright*, Proceedings of the ALAI Congress, Columbia University, New York (2002)

Goldstein, Paul, *Copyright's Highway* (revised edn, Stanford: Stanford University Press, 2003)

Gould, John, *Birds of Australia* (Part XXVI, London: John Gould, 1847)

Greenleaf, Graham, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 (5) *Privacy Law & Policy Reporter* 121

'APEC's Privacy Standard Regaining Strength' (2004) 10 (8) *Privacy Law & Policy Reporter* 158

'APEC Privacy Principles: More Lite with Every Version' (2003) 10 (6) *Privacy Law & Policy Reporter* 105

'APEC Privacy Principles Version 2 – Not Quite so Lite, and NZ wants OECD Full Strength' (2003) 10 (3) *Privacy Law & Policy Reporter* 45

'Australia's APEC Privacy Initiative: The Pros and Cons of "OECD Lite"' (2003) 10 (1) *Privacy Law & Policy Reporter* 1

'Safe Harbor's Low Benchmark for "Adequacy": EU Sells Out Privacy for US$' (2000) 7 *Privacy Law & Policy Reporter* 45

'Private Sector Bill Amendments Ignore EU Problems' (2000) 7 *Privacy Law & Policy Reporter* 41

'Global Protection of Privacy in Cyberspace – Implications for the Asia-Pacific', paper at 'Towards an Asia-Pacific Information Privacy Convention?', 1998 Internet Law Symposium, Science & Technology Law Center, Taipei, Taiwan, 23–24 June 1998, available at http://austlii.edu.au/itlaw/articles/TaiwanSTLC.html

'Stopping Surveillance: Beyond "Efficiency" and the OECD' (1996) 3 *Privacy Law & Policy Reporter* 148

'Towards an Asia-Pacific Information Privacy Convention' (1995) 2 *Privacy Law & Policy Reporter* 127

Grijpink, Jan and Prins, Corien, 'Digital Anonymity on the Internet: New Rules for Anonymous Electronic Transactions?' (2001) 17 *Computer Law and Security Report* 379

Halpern, Sheldon W., 'The "Inviolate Personality" – Warren and Brandeis After One Hundred Years' (1990) 10 *Northern Illinois University Law Review* 387

Hamelink, Cees J., *The Ethics of Cyberspace* (London, Sage: 2000)

Harris, David and Joseph, Sarah (eds.), *The International Covenant on Civil and Political Rights and United Kingdom Law* (Oxford: Clarendon Press, 1995)

Hill, John L., 'A Third Theory of Liberty: The Evolution of Our Conception of Freedom in American Constitutional Thought' (2000) 29 *Hastings Constitutional Law Quarterly* 115

Hong Kong, Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy* (Hong Kong: The Commission, December 2004)

Huff, Thomas, 'Thinking Clearly about Privacy' (1980) 55 *Washington Law Review* 777

Hugenholtz, Bernt (ed.), *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium* (The Hague: Kluwer Law International, 1996)

Hughes, Aneurin, 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)' (2001) 24 *University of New South Wales Law Journal* 270

Hughes, G. Bernard, *Victorian Pottery and Porcelain* (London: Country Life, 1959)

Kahn, Jonathan, 'Privacy as a Legal Principle of Identity Maintenance' (2003) 33 *Seton Hall Law Review* 371

Kalven, Harry, Jr., 'The New York Times Case: A Note on "The Central Meaning of the First Amendment"' 1964 *Supreme Court Review* 191

Kant, Immanuel, *The Moral Law: Kant's Groundwork of the Metaphysic of Morals*, translated and analysed by Paton, H. J. (London: Hutchinson University Library, 1948)

Katyal, Sonia K., 'The New Surveillance' (2003) 54 *Case Western Reserve Law Review* 297

Keeton, W. Page (ed.), *Prosser and Keeton on Torts* (5th edn, St Paul, Minn.: West, 1984)

Keith, Kenneth, 'A Bill of Rights: Does It Matter?' (1997) 32 *Texas International Law Journal* 393

'Democracy and a Bill of Rights for New Zealand? Judicial Review versus Democracy?' (1985) 11 *New Zealand Universities Law Review* 307

(ed.), *Essays on Human Rights* (Wellington: Sweet & Maxwell, 1968)

Kenyon, Andrew T., *Defamation: Comparative Law and Practice* (London: UCL Press, 2006)

Kerr, Ian R., 'If Left to Their Own Devices . . . How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy' in Geist, Michael (ed.), *In the Public Interest: The Future of Canadian Copyright Law* (Ottawa: Irwin Law, 2005) pp. 167–210

Keuleers, Ewout and Dinant, J. Marc, 'Data Protection: Multi-Application Smart Cards: The use of Global Unique Identifiers for Cross-Profiling Purposes – Part II: Towards a Privacy Enhancing Smart Card Engineering' (2004) 20 (1) *Computer Law and Security Report* 22

Kirby, Michael, 'Privacy Protection, A New Beginning: OECD Principles 20 Years On' (1999) 6 *Privacy Law & Policy Reporter* 25

Koelman, Kamiel J., 'Copyright Law and Economics in the EU Copyright Directive: Is the *Droit d'Auteur* Passé?' (2004) 35 (6) *International Review of Intellectual Property and Competition Law* 603

Lacey, Nicola, *A Life of H. L. A. Hart: The Nightmare and the Noble Dream* (Oxford: Oxford University Press, 2004)

Landes, William M. and Posner, Richard A., *The Economic Structure of Intellectual Property Law* (Cambridge, Mass.: Harvard University Press, 2003)

Larkin, Philip, *Collected Poems* (with introduction by A. Thwaite) (London: Marvell/Faber and Faber, 1988)

Leadbeater, Charles, *Up the Down Escalator – Why the Global Pessimists are Wrong* (London: Penguin, 2003)

Léonard, Thierry, 'E-commerce et protection des données à caractère personnel: quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet', February 2000, available at http://www.droit.fundp.ac.be/Textes/Leonard1.pdf

Lewis, Anthony, 'Privacy and Civilization' (2002) 27 *Nova Law Review* 225

Make No Law: The Sullivan Case and the First Amendment (New York: Random House, 1991)

Lichtenberg, Judith, (ed.), *Democracy and the Mass Media* (Cambridge: Cambridge University Press, 1990)

Lindsay, David, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) *Melbourne University Law Review* 179

'*Naomi Campbell* in the House of Lords: Implications for Australia' (2004) 11(1) *Privacy Law & Policy Reporter* 4

Logeais, Elisabeth and Schroeder, Jean-Baptiste, 'The French Right of Image: An Ambiguous Concept Protecting the Human Persona' (1998) 18 *Loyola of Los Angeles Entertainment Law Journal* 511

Louveaux, Sophie and Perez-Asinari, Maria Veronica, 'New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector – Some Initial Remarks' (2003) 6(5) *Computer and Telecommunications Law Review* 133

Lumby, Catherine, *Gotcha: Life in a Tabloid World* (St Leonards, NSW: Allen & Unwin, 1999)

Lumby, Catherine and Probyn, Elspeth (eds.), *Remote Control: New Media, New Ethics* (Cambridge: Cambridge University Press, 2003)

Lyon, David, *Surveillance Society: Monitoring Everyday Life* (Philadelphia: Open University, 2001)

'Everyday Surveillance: Personal Data and Social Classification' (2002) 5(2) *Information, Communication & Society* 242

McKee, Alan, *The Public Sphere: An Introduction* (Cambridge: Cambridge University Press, 2005)

MacKinnon, Catharine, *Towards a Feminist Theory of the State* (Cambridge, Mass.: Harvard University Press, 1989)

Markesinis, Basil. S. (ed.), *Protecting Privacy* (Oxford: Oxford University Press, 1999)

'Our Patchy Law of Privacy – Time to Do Something About it' (1990) 53 *Modern Law Review* 802

'The Calcutt Report Must Not Be Forgotten' (1992) 55 *Modern Law Review* 118

Markesinis, Basil S., O'Cinneide, Colm, Fedtke, Joerg and Hunter-Henin, Myriam, 'Concerns and Ideas about the Developing English Law of Privacy (and how Knowledge of Foreign Law Might Be of Help)' (2004) 52 *American Journal of Comparative Law* 133

Markesinis, Basil S. and Unberath, Hannes, *The German Law of Torts: A Comparative Treatise* (4th edn, Oxford: Hart, 2002)

May, Christopher, *The Information Society: A Sceptical View* (Cambridge: Polity, 2002)

Mayer-Schönberger, Viktor, 'The Internet and Privacy Legislation: Cookies for a Treat?' (1997) 1 *West Virginia Journal of Law and Technology* 1.1

Meiklejohn, Alexander, 'The First Amendment is an Absolute' [1961] *Supreme Court Review* 245

Michael, James, 'Privacy' in Harris, David and Joseph, Sarah (eds.), *The International Covenant on Civil and Political Rights and United Kingdom Law* (Oxford: Clarendon Press, 1995)

Michelman, Frank, 'Law's Republic' (1988) 97 *Yale Law Journal* 1493

Mill, John Stuart, *Autobiography* (London: Oxford University Press, 1971)

Utilitarianism, On Liberty, Essay on Bentham, ed. and intro. Warnock, Mary (London: Collins, 1962)

Mintz, Jonathan B., 'The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain' (1996) 55 *Maryland Law Review* 425

Moreham, N. A., 'Recognising Privacy in England and New Zealand' (2004) 63 *Cambridge Law Journal* 555

Morgan, Jonathan, 'Privacy in the House of Lords – Again' (2004) 120 *Law Quarterly Review* 563

'Privacy, Confidence, and Horizontal Effect: "Hello" Trouble' (2003) 62 *Cambridge Law Journal* 444

Morgan, Richard G., '*Roe* v. *Wade* and the Lesson of the Pre-*Roe* Case Law' (1979) 77 *Michigan Law Review* 1724

Morison, William, 'Unfair Competition and Passing Off' (1956) 2 *Sydney Law Review* 50

Muller, Jerry, *Adam Smith in His Time and Ours: Designing the Decent Society* (Princeton: Princeton University Press, 1995)

Negroponte, Nicholas, *Being Digital* (New York: Knopf, 1995)

Netanel, Neil, 'Alienability Restrictions and the Enhancement of Author Autonomy in United States and Continental Copyright Law' (1994) 12 *Cardozo Arts and Entertainment Law Journal* 1

New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report no. 98 (Sydney: NSWLRC, 2001)

New Zealand, Committee on Official Information, *Towards Open Government: General Report* (Wellington: Government Printer, 1980)

New Zealand, Committee on Official Information, *Towards Open Government, Supplementary Report* (Wellington: Government Printer, 1981)

New Zealand, Law Commission, *Evidence Law: Witness Anonymity*, NZLC R42 (Wellington: Law Commission, 1997)

New Zealand, Legislation Advisory Committee, *Report No. 8.* (Wellington: New Zealand Department of Justice, 1994)

Legislative Change: Guidelines on Process & Content (Wellington: New Zealand Department of Justice, 1991)

New Zealand, Minister of Justice, *A Bill of Rights for New Zealand – A White Paper* (1985) Appendices to the Journal of the House of Representatives, A 6

Niemann, Jan-Malte, 'Monitoring Internet and Email Usage – Germany – Surfing into Unemployment? Private Internet Use and Emailing Under German Labour Law' (2002) 18(2) *Computer Law and Security Report* 114

Nimmer, Melville B., 'The Right to Speak From *Times* to *Time*: First Amendment Theory Applied to Libel and Misapplied to Privacy' (1968) 56 *California Law Review* 935

Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, (1981) 20 ILM 422, adopted 23 September 1980

Palmer, Geoffrey, 'Privacy and the Law' [1975] *New Zealand Law Journal* 747

Parent, W. A., 'A New Definition of Privacy for the Law' (1983) 2 *Law and Philosophy* 305

Paul, Ellen, Miller, Fred, and Paul, Jeffery (eds.), *The Right to Privacy* (Cambridge: Cambridge University Press, 2000)

Pennock, J. Roland and Chapman, John W. (eds.), *Privacy* (series: Nomos XIII; New York: Atherton Press, 1971)

Phillipson, Gavin, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726

'Judicial Reasoning in Breach of Confidence Cases under the Human Rights Act: Not Taking Privacy Seriously? [2003] *European Human Rights Law Review* (Privacy Special) 53

'The Human Rights Act, "Horizontal Effect" and the Common Law: a Bang or a Whimper?' (1999) 62 *Modern Law Review* 824

Phillipson, Gavin and Fenwick, Helen, 'Breach of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 *Modern Law Review* 660

Posner, Richard A., *Overcoming Law* (Cambridge, Mass.: Harvard University Press, 1995)

'Privacy, Secrecy, and Reputation' (1979) 28 *Buffalo Law Review* 1

'The Right to Privacy' (1978) 12 *Georgia Law Review* 293

Post, Robert C., 'Meiklejohn's Mistake: Individual Autonomy and the Reform of Public Discourse' (1993) 64 *University of Colorado Law Review* 1109

'Rereading Warren and Brandeis: Privacy, Property, and Appropriation' (1991) 41 *Case Western Law Review* 647

'The Social Foundations of Privacy: Community and Self in the Common Law Tort' (1989) 77 *California Law Review* 957

Poullet, Yves, 'Making Data Subjects Aware of Their Rights and Capable of Protecting Themselves', Conference on the Rights and Responsibilities of Data Subjects, Council of Europe, Prague, 14–15 October 2004 (being published)

Poullet, Yves and Dinant, J. Marc, *Information Self-Determination in the Internet Era: Thoughts on Convention No. 108 for the Purposes of the Future Work of the Consultative Committee*, 13 December 2004 (T-PD (2004) 04 final)

Pound, Reginald, *Albert: A Biography of the Prince Consort* (London: Michael Joseph, 1973)

Prescott, Peter, '*Kaye* v. *Robertson* – A Reply' (1991) 54 *Modern Law Review* 451

Prosser, William L., 'Privacy' (1960) 48 *California Law Review* 383

Rachels, James, 'Why Privacy is Important' (1975) 4 *Philosophy and Public Affairs* 323

Rasky, H. L., 'Can an Employer search the Contents of his Employees' E-mail?' (1998) 20 *Advocates' Quarterly* 221

Raz, Joseph, 'Free Expression and Personal Identification' (1991) 11 *Oxford Journal of Legal Studies* 303

Reidenberg, Joel R., 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review* 1315

Reiman, Jeffrey H., 'Privacy, Intimacy, and Personhood' (1976) 6 *Philosophy and Public Affairs* 26

Richardson, Megan, 'Privacy and Precedent: The Court of Appeal's Decision in *Hosking* v. *Runting*' (2005) 11 *New Zealand Business Law Quarterly* 82

'Whither Breach of Confidence: A Right of Privacy for Australia?' (2002) 26 *Melbourne University Law Review* 381

Robertson, Andrew (ed.), *The Law of Obligations: Connections and Boundaries*, (London: UCL Press, 2004)

Rodota, Stefano, 'Beyond the EU Directive: Directions for the Future' in Poullet, Yves, de Terwangne, Cécile and Turner, Paul (eds.), *Privacy: New Risks and Opportunities*, Cahier du CRID no. 13 (Antwerpen: Kluwer, 1997)

Rogers, Heather and Tomlinson, Hugh, 'Privacy and Expression: Convention Rights and Interim Injunctions' [2003] *European Human Rights Law Review* (Privacy Special) 37

Rorty, Richard, *Philosphy and Social Hope* (London: Penguin, 1999)

Contingency, Irony, and Solidarity (Cambridge: Cambridge University Press, 1989)

Rotenberg, Marc, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' [2001] *Stanford Technology Law Review* 1

Rozenberg, Joshua, *Privacy and the Press* (revised edn, Oxford: Oxford University Press, 2005)

Rubenfeld, Jed, 'The Right of Privacy' (1989) 102 *Harvard Law Review* 737

Sack, Robert D., *Sack on Defamation: Libel, Slander, and Related Problems* (3rd edn, New York City: Practising Law Institute, 1999)

Sanderson, M. A., 'Is *Von Hannover* v. *Germany* a Step Backward for the Substantive Analysis of Speech and Privacy Interests?' (2004) 6 *European Human Rights Law Review* 631

Schauer, Frederick, 'The Exceptional First Amendment' in Ignatieff, Michael (ed.), *American Exceptionalism and Human Rights* (Princeton: Princeton University Press, 2005)

Free Speech: A Philosophical Enquiry (Cambridge: Cambridge University Press, 1982)

'Reflections on the Value of Truth' (1991) 41 *Case Western Reserve Law Review* 699

Schnably, Stephen J, 'Beyond Griswold: Foucauldian and Republican Approaches to Privacy' (1991) 23 *Connecticut Law Review* 861

Schneider, Elizabeth, 'The Violence of Privacy' (1991) 23 *Connecticut Law Review* 973

Schoeman, Ferdinand (ed.), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984)

Schwartz, Paul M., 'Beyond Lessig's Code for Internet Privacy: Cyberspace, Filters, Privacy Control and Fair Information Practices' (2000) *Wisconsin Law Review* 749

Seipel, Peter, 'Information System Quality as a Legal Concern' in Gasser, Urs (ed.), *Information Quality Regulation: Foundations, Perspectives, Applications* (Baden-Baden: Nomos, 2004)

(ed.), *Law and Information Technology: Swedish Views*, Swedish Government Official Reports, SOU 2002: 112

Sheppard, Annamay T., 'Thoughts on *Bowers* v. *Hardwick*' (1988) 40 *Rutgers Law Journal* 521

Sherborne, David and Jethani, Sapna, 'The Privacy Codes' in Tugendhat, Michael and Christie, Iain (eds.), *The Law of Privacy and the Media* (Oxford: Oxford University Press, 2002) and *First Cumulative Updating Supplement* (2004)

Sherman, Brad and Bently, Lionel, *The Making of Modern Intellectual Property Law* (Cambridge: Cambridge University Press, 1999)

Sherman, Brad and Strowel, Alain, *Of Authors and Origins* (Oxford: Clarendon Press, 1994)

Skone James, Francis E., *Copinger on the Law of Copyright* (6th edn, London: Sweet & Maxwell, 1927)

Smith, Joseph H. and Kerrigan, William (eds.), *Pragmatism's Freud* (Baltimore: Johns Hopkins University Press, 1986)

Smolla, Rodney A., *Smolla & Nimmer on Freedom of Speech* (3rd edn, New York: Clark Boardman Callaghan, 1996–2005)

'Accounting for the Slow Growth of American Privacy Law' (2002) 27 *Nova Law Review* 289

'Information as Contraband: The First Amendment and Liability for Trafficking in Speech' (2002) 96 *Northwestern University Law Review* 1099

Tang, Raymond, 'Personal Data Privacy: The Asian Agenda', paper at 25th International Conference of Data Protection and Privacy Commissioners, Sydney, 10–12 September 2003, available from http://www.pco.org.hk

Taylor, Charles, *The Ethics of Authenticity* (Cambridge, Mass.: Harvard University Press, 1992)

de Terwangne, Cécile, 'Affaire *Lindqvist* ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles' (2004) 19 *Revue du Droit des Technologies de l'Information* 67

Thomas, Kendall, 'Beyond the Privacy Principle' (1992) 92 *Columbia Law Review* 1431

Thompson, John B., *Political Scandal: Power and Visibility in the Media Age* (Cambridge: Polity Press, 2000)

Tugendhat, Michael and Christie, Iain (eds.), *The Law of Privacy and the Media* (Oxford: Oxford University Press, 2002) and *First Cumulative Updating Supplement* (2004)

Tullock, Gordon, *The Economics of Special Privilege and Rent Seeking* (Dordrecht: Kluwer, 1989)

Tully, James (ed.), *Philosophy in an Age of Pluralism* (Cambridge: Cambridge University Press, 1994)

Turkington, Richard, 'Confidentiality Policy for HIV-Related Information: An Analytic Framework for Sorting Out Hard and Easy Cases' (1989) 34 *Villanova Law Review* 871

Turner, Graeme, *Ending the Affair: The Decline of Television Current Affairs in Australia* (Sydney: University of NSW Press, 2005)

Understanding Celebrity (London: Sage, 2004)

Turner, Graeme, Bonner, Frances and Marshall, P. David, *Fame Games: The Production of Celebrity in Australia* (Melbourne: Cambridge University Press, 2000)

United Kingdom, Committee on Homosexual Offences and Prostitution, *Report of the Committee on Homosexual Offences and Prostitution* (London: HMSO, 1957)

United Kingdom, Home Office, *Report of the Committee on Privacy and Related Matters*, Cm 1102 (London: HMSO, 1990)

United Kingdom, House of Commons, Culture, Media and Sport Committee, *Privacy and Media Intrusion*, Fifth Report of Session 2002–03, HC 458-I

United Kingdom, Ofcom, *Ofcom Review of Public Service Television Broadcasting: Phase 2 – Meeting the Digital Challenge* (London: Ofcom, 2004)

United Nations, Human Rights Committee, *Concluding Observations of the Human Rights Committee: New Zealand*, CPR/CO/75/NZL, 26 July 2003

Concluding Observations of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland, CCPR/CO/73/UK, CCPR/CO/73/UKOT, 6 December 2001

United States, Committee on Intellectual Property Rights and the Emerging Information Infrastructure, *The Digital Dilemma* (Washington, DC: National Academy Press, 2000)

United States, Congressional Budget Office, *Copyright Issues in Digital Media* (Washington, DC: CBO, August 2004)

United States, Federal Trade Commission, *Prepared Statement of the Federal Trade Commission on 'Privacy Online: Fair Information Practices in the Electronic Marketplace'* (May 2000)

United States, Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights Information Infrastructure Task Force* (Washington, DC: United States Department of Congress, 1995)

Van Wassenhove, Stanislas, De Leersnyder, Michael and Chuffart, Gael, *Nouvelles technologies et impact sur le droit du travail* (Kortrijk-Heule: UGA, 2003)

Wacks, Raymond, *Law, Morality, and the Private Domain* (Hong Kong: Hong Kong University Press, 2000)

'What has Data Protection to do with Privacy?' (2000) 6 *Privacy Law & Policy Reporter* 143

'Towards a New Legal and Conceptual Framework for the Protection of Internet Privacy' (1999) 3 *Irish Intellectual Property Review* 1

'Privacy and Press Freedom: Oil on Troubled Waters' (1999) 4 *Media & Arts Law Review* 259

'Privacy and Media Intrusion: A New Twist' (1999) 6 *Privacy Law & Policy Reporter* 48

'Media Intrusion: An Expanded Role for the Privacy Commissioner?' (1999) 29 *Hong Kong Law Journal* 341

'Pursuing Paparazzi: Privacy and Intrusive Photography' (1998) 1 *Hong Kong Law Journal* 1

Privacy and Press Freedom (Oxford: Oxford University Press, 1995)

Personal Information: Privacy and the Law (Oxford: Clarendon Press, 1993)

(ed.), *Privacy: Volume I* (Aldershot: Dartmouth; New York: New York University Press, 1993)

'Controlling AIDS: Some Legal Issues' (1988) 138 *New Law Journal* 254 and 283.

The Protection of Privacy (London: Sweet & Maxwell, 1980)

'The Poverty of "Privacy"' (1980) 96 *Law Quarterly Review* 73

Wade, H. W. R., 'Horizons of Horizontality' (2000) 116 *Law Quarterly Review* 217

Wallace, Amy, *The Prodigy* (New York: E. P. Dutton, 1986)

Warren, Samuel D. and Brandeis, Louis D., 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193

Waters, Nigel, 'Rethinking Information Privacy – A Third Way in Data Protection?' (2000) 6 *Privacy Law & Policy Reporter* 121

Weaver, Russell L., Kenyon, Andrew T., Partlett, David F. and Walker, Clive P., *The Right to Speak Ill: Defamation, Reputation and Free Speech* (Durham, NC: Carolina Academic Press, 2006)

Wellek, Rene (ed.), *The Attack on Literature and Other Essays* (Chapel Hill: University of North Carolina Press, 1982)

Wermiel, Stephen J., 'Law and Human Dignity: The Judicial Soul of Justice Brennan' (1998) 7 *William and Mary Bill of Rights Journal* 223

Westin, Alan, *Privacy and Freedom* (London: Bodley Head, 1967)

White, Antony, 'Data Protection and the Media' [2003] *European Human Rights Law Review* (Privacy Special) 25; volume also published as Cooper, Jonathan (ed.) *Privacy* (London: Sweet and Maxwell, 2003)

White, Stephen K., *Sustaining Affirmation: The Strengths of Weak Ontology in Political Theory* (Princeton: Princeton University Press, 2000)

Whitman, James Q., 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151

Wilson, A. N., *The Victorians* (London: Arrow Books, 2003)

Woodmansee, Martha and Jaszi, Peter, *The Construction of Authorship: Textual Appropriation in Law and Literature* (Durham: Duke University Press, 1994)

Young, John B. (ed.), *Privacy* (New York: Wiley, 1978)

Zammit, Brigitte, 'Traffic Data Retention under EC Law' (2005) 11(1) *Computer and Telecommunications Law Review* 17

Zimmerman, Diane L., 'Requiem for a Heavyweight: a Farewell to Warren and Brandeis's Privacy Tort' (1983) 68 *Cornell Law Review* 291

INDEX

INDEX OF LAWS AND DIRECTIVES

International

European

Australia

Belgium

Canada

Germany

New Zealand

Sweden

UK

US

Asia

INDEX OF CASE REFERENCES

France

Germany

Iceland

New Zealand

Spain

Sweden

UK

US