1

An overview of emerging challenges in privacy law

NORMANN WITZLEB, DAVID LINDSAY, MOIRA PATERSON AND SHARON RODRICK

Privacy holds a highly contested place within contemporary political and legal discourse. One of the difficulties associated with privacy claims is the relatively amorphous nature of privacy. As Robert Gellman aptly said:

> Lawyers, judges, philosophers, and scholars have attempted to define the scope and meaning of privacy, and it would be unfair to suggest that they have failed. It would be kinder to say that they have all produced different answers.[1]

Particularly marginal or novel claims for privacy are sometimes resisted with the argument that privacy is meaningless when it potentially encompasses all and any claims to individual liberty and autonomy. Yet it should no longer be doubted that privacy is a fundamental concern and that, in many traditional settings, it has also acquired a fairly specific scope and meaning. However, privacy is difficult to enforce because it is not an absolute right. Its protection must always be sought against conflicting values or interests. While the conflict between privacy and freedom of expression has been a constant for many decades, it is becoming apparent that public safety and national security concerns have resurged as the nemesis of privacy claims, in particular when states consider themselves under siege from external and internal threats.

At the time of writing, that is perfectly illustrated by the public debates surrounding the revelations of former CIA employee Edward Snowden concerning the US National Security Agency's (NSA's) 'Operation PRISM', under which the NSA obtained access to large amounts of communications data concerning non-US citizens held by Google, Facebook, Apple,

[1] R. Gellman, 'Does Privacy Law Work?' in Philip Agre and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape* (Cambridge, MA: MIT Press, 1997), p. 193.

Verizon and other Internet companies.[2] These debates raise serious questions about the power relations between national governments, private corporations and individuals, which lie at the very heart of socio-political life. The Snowden revelations illustrate that the digitisation of modern communications makes it possible for governments to collect vast amounts of data on their citizens and, indeed, many others around the globe. Even when these communications data do not extend to the content of communications, they reveal patterns of our interactions with others, our physical locations or informational habits that can, if gathered, stored, retrieved and cross-referenced, expose our personalities and private lives in unprecedented detail. Needless to say, corporations are keen to use the same or similar technologies to gauge consumer habits with the objective of personalising advertising. It may be that the implications of emerging privacy-invasive technologies and surveillance practices – including, for example, the mining of 'big data'[3] – are so great that we have yet to develop adequate analytical frameworks.[4] Clearly, rapid technological developments are a major driver of the current concern with 'privacy'. Increasingly sophisticated equipment is providing us with ever-greater ability at ever-lower cost to invade the privacy of others. Such means, be they high-performing cameras, GPS trackers or online tracking and data analysis technologies, are not at the disposal just of the state and large media organisations; they are often in the hands of ordinary citizens.

These technological developments have coincided with significant social change affecting the notion of privacy. The advent of social media has given everyone a forum in which to disclose personal information on a large and permanent scale, and many do so readily, at times to their subsequent regret. The pervasiveness of social media has challenged individual and societal views of what is, or should be, private. Indeed, self-revelation of information that the vast majority of citizens would have once taken pains to conceal are now commonplace. This may also be a reason why there is now a greater expectation that private information about others *will* be disclosed. However, it is inherent in the notion of

[2] G. Greenwald and E. MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others', *Guardian* (Online) 7 June 2013, www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data (accessed 5 October 2013).

[3] See, for example, V. Mayer-Schönberger and K. Cukier, *Big Data* (London: John Murray, 2013).

[4] For a recent debate concerning how best to conceptualise the harms of widespread surveillance see: N. M. Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934; D. Keats Citron and D. Gray, 'Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards' (2013) 126 *Harvard Law Review Forum* 262.

privacy that, in principle, each person maintains control over how much of their personal information becomes available to others and to whom it should become known. While the migration of peoples' social lives to the online environment has affected perspectives of what is 'public' and what is 'private', this has made it more, rather than less significant that societies protect individual preferences concerning what private information *should* become accessible to others.

Despite the rapid emergence of social media, the more traditional mass media remain an important focus of privacy concerns. Media convergence and the rise of social media have affected the work and ethics of the mass media. The advent of the twenty-four-hour news cycle and increasing commercial pressures have contributed to declining standards in the media and spawned an increased reliance on infotainment and sensational reporting, both of which have implications for privacy. This includes the cult of the celebrity, which is now part of the fabric of developed societies. Typical targets of the public's thirst for information about the private lives of others include members of royal families, entertainers, high-profile sportspersons and 'ordinary' persons who, through choice or accident, come to public attention. Information that in the past would not have been published in the mass media may now feature on social media, thereby creating 'news' that may then be taken up and be more broadly disseminated by the traditional media. This has created an interdependent relationship between social media and mass media; moreover, it is breaking down the barriers between them.

The focus of this book is not, however, primarily on these significant technological and social developments. Instead, the essays in this collection are concerned with the current and emerging legal challenges that arise from these developments. While acknowledging the considerable cultural and social differences between jurisdictions, an important feature of the legal landscape internationally is the increasing recognition of privacy as a human right. A number of significant treaties and conventions, including the International Covenant on Civil and Political Rights (ICCPR) and the Convention for the Protection of Human Rights and Fundamental Freedoms, generally known as the European Convention on Human Rights (ECHR), recognise respect for private and family life as a fundamental human right. The constitutions of many countries, such as the USA and Germany, enshrine a list of human rights. Other countries, such as Canada or New Zealand, have enacted legislation containing bills of rights or have adopted an international human rights instrument as part of their domestic law. The enactment of the Human Rights Act 1998

(UK), which incorporated the ECHR into UK domestic law, is a prime example of the latter. There remain, nevertheless, considerable differences in how privacy is protected at the level of domestic law.

It is universally acknowledged that the complex European human rights framework has been developed to provide the highest level of legal protection of the rights to privacy and data protection.[5] The importance placed on these rights in Europe is illustrated not merely by significant judgments of the European Court of Human Rights but by the recent European Commission proposal for a new data privacy instrument, which is intended to address the challenges posed by the increased collection and processing of personal data online, including the emergence of social networking services.[6] By comparison, the United States provides relatively weak and patchy protection, partly due to the constitutional emphasis placed on freedom of expression and partly due to an entrenched cultural preference for market-based solutions.[7] Most other Western-oriented jurisdictions lie somewhere between these two ends of the spectrum. Australia, for example, is the only Western democracy that lacks significant constitutional or statutory protection of human rights and, as Greenleaf has pointed out:

> Australia has … had twenty years' involvement in developing international privacy standards as an influential non-EU participant. Its chosen role has been to advocate privacy protection as a legitimate and unavoidable issue, but one that can be managed in the interests of business and government, rather than advocacy of privacy as a human right.[8]

Most jurisdictions pay lip service to the need for legal protection of the right to privacy, especially in response to the technological and social threats mentioned above. Yet it must be acknowledged that its protection

[5] For further detail, see P. Hustinx, Chapter 4 (in this volume) and U. Fink, Chapter 5 (in this volume).

[6] See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (GDPR) (Brussels, 25 January 2012) 2012/0011(COD).

[7] See, for example, J. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151; D. Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131.

[8] G. Greenleaf, 'Country Studies B.2 – AUSTRALIA' in D. Korff (ed.), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments* (Brussels: European Commission D-G Justice, Freedom and Security, 2010).

cannot be absolute and that countervailing rights and interests may sometimes trump privacy. We have already referred to the classic conflicts between privacy and public safety and national security, and between privacy and freedom of expression. The work of courts and parliaments, assisted by law reform agencies, civil society academic commentators and the media in setting this equilibrium provides the true test for how adequately a society protects the privacy of its citizens.

This book of essays has its origins in a research project funded under the Go8 Germany Joint Research Co-operation Scheme. Grant-holders under this scheme, which is a joint initiative of the Group of Eight (Go8) and the German Academic Exchange Service (DAAD), were the editors, together with Professors Udo Fink and Dieter Dörr, Dr Stephanie Schiedermair and Dr Eva Aernecke, all from the Johannes-Gutenberg-Universität in Mainz. The project culminated in a two-day international conference on 'Emerging Challenges to Privacy Law: Australasian and EU Perspectives', which took place in February 2012 at the Monash University Law Chambers in Melbourne/Australia. Many of the papers presented at that conference have been revised and adapted for inclusion in this book. Others do not have their genesis as conference papers but were specifically commissioned for the present collection.

Part I: Reforming the data protection frameworks: Australian and EU perspectives

Part I of the collection provides an overview of the current data privacy reform processes in Europe and Australia, from the perspective of those with 'hands-on' experience with the administration and enforcement of the relevant laws. Contributors include the Australian Privacy Commissioner and the European Data Protection Supervisor.

In Chapter 2 of the book, Timothy Pilgrim, the Australian Privacy Commissioner, addresses the challenges and opportunities facing privacy law reform from an Australian perspective. After acknowledging the importance of recognising privacy as a fundamental right, Pilgrim reviews the recent history of Australian law reform, which centres on the landmark 2008 report by the Australian Law Reform Commission (ALRC)[9] and the Australian Federal Government's response to that report. As Pilgrim explains, partly due to the large number of recommendations made by the

[9] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report no. 108 (2008).

ALRC, the Australian Government decided to respond to the report in two stages (or 'tranches').

The first stage of the reforms, enacted via the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), includes the introduction of a single set of privacy principles to apply across the public and private sectors, reforms to the credit-reporting provisions and new powers for the Privacy Commissioner. It may be that the additional enforcement powers given to the Commissioner will encourage a greater emphasis on enforcement than has been the case in Australia, where to date there has been a preference for conciliation of privacy disputes over formal determinations by the Privacy Commissioner. After a review of some of the enforcement activities in high-profile cases in the USA, the UK and France, Pilgrim makes it clear that the Commissioner is prepared to make enforceable determinations, at least in the case of serious breaches. The chapter also confirms that there is a new emphasis on transparency, with the publication of investigation reports of serious or high-profile breaches.

Given the global or transborder nature of many contemporary privacy threats, a key challenge facing data protection authorities is deciding when entities based outside a territorial jurisdiction are, nevertheless, within their jurisdictional reach. Pilgrim explains some of the difficulties that arise from applying the Privacy Act 1988 (Cth) extraterritorially, using the example of the Commissioner's investigation into the large-scale unauthorised release of personal data by the Sony PlayStation Network in 2010. Later in the chapter, the author returns to this issue to emphasise the importance of initiatives encouraging cross-border collaboration between privacy regulators, such as the Global Privacy Enforcement Network and the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement. Pilgrim points out that the Sony investigation also revealed the heightened vulnerability of networked electronic records to massive data breaches. Among the future challenges for Australian privacy law reform, Pilgrim identifies two issues set aside for the second stage of the government's response to the ALRC report: the exemptions from the Australian data privacy law, including the exemption for small businesses; and the recommendation for introducing a statutory cause of action for serious invasions of privacy. While the government has yet to respond to the ALRC's recommendations to remove exemptions, the Commonwealth Attorney-General has issued a reference to the ALRC for an inquiry into 'Serious Invasions of Privacy in the Digital Era', which, in part, will produce recommendations

regarding the 'detailed legal design of a statutory cause of action for serious invasions of privacy'.[10]

In Chapter 3, Nigel Waters reviews the privacy law reform process from the perspective of an experienced Australian privacy advocate. As Waters points out, the key issues facing law reform in Australia are shared by all data privacy regimes. These include new business models and practices, new actors, jurisdictional problems and enforcement issues. New online business models tend to create complex new relationships between multiple parties, often with limited transparency in how personal data will be collected and used. This creates obvious challenges for writing privacy policies, which are exacerbated by the limitations of screen displays, especially on mobile devices. New applications, including social networking, have given individuals the ability to collect and process considerable amounts of personal data; yet, as Waters points out, there are significant uncertainties about applying data privacy laws to the actions of private individuals. The liability of intermediaries for data processing, whether under Australian or European law, also raises difficult issues.

The analysis of recent Australian privacy law reform undertaken by Waters provides a counterpoint to Pilgrim's account of the reform process. Waters observes that in 2010, as the government was responding to the ALRC report, the Office of the Privacy Commissioner was combined with the freedom of information and information policy roles of the Federal Government to form the Office of the Australian Information Commissioner (OAIC). This administrative reorganisation resulted in internal tensions and potential distractions from the reform process. Waters further maintains that the consultation process associated with the first stage of the privacy law reforms resulted in the watering-down of privacy protections, including weaker privacy principles, yet increased their legal complexity. Although not expressly raised by Waters, this may suggest that, in a regime that fails to recognise privacy as a fundamental right, it may be more difficult to resist commercial interests seeking to influence the policy process in their favour. Waters also comments on the new enforcement powers for the Privacy Commissioner, as discussed in Pilgrim's chapter. While generally welcoming the new powers, he points to a major omission: as complainants have no right to a formal decision, enforcement remains within the discretion of the Privacy Commissioner.

[10] M. Dreyfus, Commonwealth Attorney-General, *Terms of Reference: Serious Invasions of Privacy in the Digital Era* (12 June 2013), www.alrc.gov.au/inquiries/invasions-privacy (accessed 8 November 2013).

In Waters' experience of the Australian regime, the effective protection of data privacy requires more prescriptive laws and more active enforcement. Yet, on both these elements, the recent Australian reforms fall short of the expectations of privacy advocates.

In Chapter 4, Peter Hustinx, the European Data Protection Supervisor, provides an overview of the EU data privacy reform process, which culminated in the release of drafts of proposed reforms in January 2012. In contrast to the position in Australia, the European reform process can take the human rights guarantees of the right to privacy as its starting point. However, as Hustinx points out, the European data privacy laws historically developed largely as a response to the limitations of the right to private life (in Article 8 of the ECHR) in dealing with large-scale automated processing of personal data in the 1970s. The rights-based orientation of the European regime was reinforced by the adoption of the European Charter of Fundamental Rights[11] (the 'Charter') in 2000 and, subsequently, the Lisbon Treaty[12] in 2009, which both explicitly recognise a distinct fundamental right to data protection.

Since the introduction of European data privacy laws in the 1970s, the objective of harmonised protection at the European level has been frustrated by persistent disparities between national data protection regimes. As the chapter explains, disparities between the national implementations of Directive 95/46/EC[13] have resulted in unnecessary costs and diminished effectiveness of the European framework. Hustinx identifies the need for greater harmonisation as one of the drivers of the current reform process, the other two being the need to update the law, especially to take into account internet-related technological developments, and the requirement to comply with the Charter and the Lisbon Treaty. The reforms, as released in January 2012, consist of two proposed instruments: a directive relating to the processing of personal data by law enforcement authorities,[14] which must be implemented in EU member states; and a General

[11] Charter of Fundamental Rights of the European Union [2010] OJ C 83/02.

[12] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, signed 13 December 2007, [2007] OJ C 306/1 (entered into force 1 December 2009).

[13] 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.

[14] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data* (Brussels, 25 January 2012) 2012/0010(COD).

Data Protection Regulation (GDPR),[15] which has direct effect in member states. The proposed GDPR builds on Directive 95/46/EC but clarifies and increases the level of data protection, and enhances enforcement. The chapter identifies the main ways in which the GDPR increases protection, which are as follows: enhancing user control, including increasing the threshold for consent and a stronger right to object; clarifying and tightening the responsibilities of data processors, including requirements for privacy impact assessments; and providing a greater emphasis on supervision and enforcement, including increased enforcement powers for national regulators and a mechanism for ensuring consistency between national regulators in their supervision and enforcement activities. Finally, the chapter explains how the proposed GDPR addresses the challenges of internet-based globalisation of data processing by means of clarifying and extending the rules relating to transborder data flows, and including a specific provision on Binding Corporate Rules.

Together, the three perspectives offered in the chapters collected in Part I reveal a degree of agreement on the challenges facing data privacy law reform. For example, globalisation of data processing and the widescale use of internet-based applications make it urgent for data protection laws to address issues relating to extraterritorial application and enforcement. Although there is agreement on the need for cooperation between national regulators, there is less agreement on the substantive rules to apply to transborder data processing, or the circumstances in which extraterritoriality is justified. It is notable that each of the chapters in this Part emphasises the importance of adequate enforcement of data protection laws. The European regime has been criticised as being strong on the books but weak on practical enforcement. However, as Nigel Waters explains, the reticence to issue binding determinations has also been identified as a key weakness of the Australian law. The relatively disappointing track record of enforcement in Australia and parts of Europe raises questions as to how to ensure the effective use of new enforcement powers. From a broader perspective, the importance placed on the right to data protection within the European legal framework has clearly influenced the extremely ambitious nature of the current European reform process. By comparison, law reform in Australia has been timid and tentative, with the most difficult and controversial challenges effectively postponed to some point in the future. The centrality of data processing to the global knowledge economy, and to the business models of powerful stakeholders, has made serious law reform a

[15] European Commission, GDPR, above n. 6.

complex, controversial and protracted endeavour. At the time of writing, it remains to be seen whether the current law reform processes in Europe and Australia will indeed substantially enhance data protection regimes against vested business and governmental interests.

Part II: Privacy in European human right instruments

In Chapter 5, Udo Fink explains the architecture of privacy protection in Europe and, more specifically, the European Union, and in this way builds upon the material introduced by Peter Hustinx. The most influential legal instrument for privacy rights is the ECHR, which in its Article 8 guarantees the right to private and family life. All member states of the EU, indeed all members of the Council of Europe, have ratified the ECHR. Apart from binding each member state, it also forms part of the general principles of EU law and, in addition, the EU itself is now in the process of acceding to the ECHR. The European Union now also has its own human rights instrument in the form of the Charter. With the entry into force of the Lisbon Treaty on 1 December 2009, the Charter has become legally binding. The Charter, which sets out fundamental rights that reflect Europe's common values and its constitutional heritage, contains two relevant provisions on privacy and data protection. Article 7 of the Charter protects private and family life, home and communications, and thus has a similar reach to Article 8 of the ECHR. In addition, Article 8 of the Charter specifically protects personal data, restricting the member states' ability to collect and process such data, providing rights to access and rectification, and requiring that an independent authority can be called upon to control compliance with these obligations.

Fink then analyses the most important aspects of the jurisprudence of the European Court of Human Rights on Article 8 of the ECHR. The Strasbourg Court has a strong tradition of protecting privacy and its jurisprudence is influential beyond Europe. A broad understanding of 'private life' has enabled the Court to utilise Article 8 in rulings on the legality of bodily searches, homosexual activity and other aspects of a person's intimate life. In the absence of a more specific provision, Article 8 is also relevant for data protection. The Strasbourg Court has also made some important decisions on the protection of privacy against the media. Of particular significance is the 2004 decision in *Von Hannover* v. *Germany*[16] (known

[16] *Von Hannover* v. *Germany* (Application no. 59320/00) [2004] ECHR 294, (2005) 40 EHRR 1.