Article

Is data protection the new privacy?

by Megan Richardson

Is data protection the new privacy? Over a century ago the Bostonians Samuel Warren and Louis Brandeis argued that traditional (US) legal doctrines were inadequate to deal with modern concerns about privacy which had emerged alongside the use of new surveillance technologies such as the "instantaneous photographs" and the media practices of the yellow press ("The right to privacy", (1890) 4 *Harvard Law Review* 193). Their argument for legal recognition of "the right to privacy", defined as a right to be "let alone" and characterised as a right of "inviolate personality", gave rise to a century of tort law reform in the United States. Already, by 1960, as William Prosser said, torts of intrusion on seclusion, public disclosure of private facts, false light publicity and misappropriation of name or likeness could be identified as falling within the general rubric of privacy torts ("Privacy", (1960) *California Law Review* 383). Moreover, notwithstanding the absence of any explicit reference to a constitutional right to privacy in the US Bill of Rights, the Supreme Court has treated privacy as underpinning aspects of the Bill's enumerated rights in cases such *Roe v Wade*, 410 US 113 (1973) and *Lawrence v Texas*, 539 *US* 558 (2003) (fourteenth amendment right of due process as applied to laws against abortion and sodomy), *Bartnicki v Vopper*, 532 US 514 (2001) (first amendment right of free speech as applied of private disclosure), and *Katz v United States*, 389 *US* 347 (1967) and *United States v Jones*, 565 US ___, 132 SCt 945 (2012) (fourth amendment restrictions on search and seizure applied to private material).

The 20th century American approach of emphasising privacy as a key concept shaping doctrinal development and constitutional discourse has also expanded into other common law jurisdictions. The constitutional dimension may be less overt (with the partial exception of the Canadian Charter of Rights and Freedoms of 1982, where privacy has had a significant shaping effect on the s 8 search and seizure clause). But a growing emphasis on privacy has been evident in the reform of private law doctrine especially in the courts. In more conservative jurisdictions, such as Australia, courts have been largely content so far to see their traditional doctrines develop in ways that accord with privacy. However, in more progressive jurisdictions courts have gone further to fashion their own privacy torts, taking the US jurisprudence as a model in whole or part. For instance, a public disclosure of private facts tort was recognised by the New Zealand Court of Appeal in *Hosking v Runting* [2005] NZLR 1. And an intrusion on seclusion tort became the basis for the Ontario Court of Appeal in *Jones v Tsige*, 2012 OJ No 148 to deal with the defendant's surreptitious electronic surveillance of the plaintiff's bank records. (A New Zealand court recognised a similar tort in *C v Holland* NZHC 2155). More generally, as Sharpe JA observed in *Jones v Tsige*:

> *Canadian, English and American courts and commentators almost invariably take the seminal articles of S D Warren & L D Brandeis, "The Right to Privacy", (1890) 4 Harv L R 193 and William L Prosser, "Privacy" (1960), 48 Cal L R 383 as their starting point. ([2012] OJ No 148 at [16])*

England however has been more influenced by a longer tradition of privacy protection in Continental Europe, which Warren and Brandeis acknowledged as an influence on their own arguments for direct legal protection of privacy in the US in 1890 – noting that "the right to privacy ... has already found expression in the law of France" (4 *Harvard Law Review* at 214). There is still no general privacy doctrine in this jurisdiction. That was apparently ruled out by the House of Lords in *Wainwright v Home Office* [2004] 2 AC 406. But in the wake of the Human Rights Act 1998 giving effect to the European Convention on Human Rights 1950, including its article 8 right to "private life", a substantial English jurisprudence has developed towards acknowledging a tort of misuse of private information as an outgrowth of the traditional doctrine of breach of confidence. As the "new methodology" is explained in *McKennitt v Ash* [2008] QB 73, *Murray v Express Newspapers Plc* [2009] Ch 481 and *Mosley v Newsgroup Newspapers Ltd* [2008] EWHC 1777 (QB), the tort responds directly to the United Kingdom's obligation to respect the right to private life in article 8 of the ECHR.

But now in Europe there is a new legal concept being talked of which is said to represent a step beyond privacy and which has also been declared the subject of a fundamental right. That is the right to "protection of personal data" in article 8 of the Charter of Fundamental Rights of the European Union 2000. According to the Treaty of Lisbon 2007, which finally came into force in December 2009, this is part of the constitutional fabric of the European Union. Is a right to data protection a hyperbolic statement, a reflection of an over-expansion of rights in the post-human rights era, leading to a fragmentation

of the very idea of "a right" – as eloquently noted in the Beastie Boys' sarcastic refrain "you gotta fight for your right to party"? Or is language of a right to data protection rather a prediction that data protection will eventually supersede privacy as the preferred legal technology of the information age?

There is much to suggest the latter. The Charter's article 8 right to data protection is identified as a basis for the EU's current draft Data Protection Regulation 2012. That this has been framed with the internet especially in mind is clear from the provisions dealing with tracking, profiling, data portability and correction and erasure of data files (the so-called "right to be forgotten") (see arts 16-20). Individuals who suffer damage from violation of these standards may seek compensation in court (see art 78). But perhaps more importantly data protection commissioners and their offices have significant powers of their own, including the power to award penalties of up to € million or 2 per cent of annual worldwide turnover of companies that fail to comply (see arti 77) – a not insignificant amount. Interestingly, there is no reference in the draft Regulation to the right to private life, although the Charter itself mentions the right to "respect for private life" in article 7.

Although the draft Regulation is yet to become law, the right to data protection in the EU Charter is shaping the European legal landscape. The right was noted, for instance, by the European Court of Justice as a reason to limit the making of general judicial orders requiring internet service providers and online social networks to monitor their users' communications for possible copyright infringements in the cases of *Scarlet Extended SA* v *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* (CJ, Third Chamber, C-70/10, November 24, 2011) and *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v *Netlog NV* (CJ, Third Chamber, C-360/10, February 16, 2012), both referred from Belgian courts. Further, the international anti-counterfeiting trade agreement ACTA was rejected by the European Parliament in July 2012, exercising its powers under the Lisbon Treaty, after the European Data Protection Supervisor issued an opinion in April that its measures may operate in breach of articles 7 and 8 of the EU Charter as well as article 8 of the ECHR (see http://europa.eu/rapid/press-release_EDPS-12-9_en.htm).

Already, existing data protection standards prescribed by the EU's Data Protection Directive 1995 have had a significant effect in continental European jurisdictions, where data protection laws were often in place even before the Directive. In particular, data protection authorities and courts in Germany and France and other continental jurisdictions have used their powers for a range of purposes in recent years, including with respect to Facebook, Google and Twitter and the like. Even in England, where the influence of the European-prescribed standards has been less pronounced (and Lisbon strictly speaking will not change that, given the UK's reservation that the Charter rights should not alter domestic law) there are tentative suggestions of a growing importance being accorded to data protection. For instance, section 35 of the Data Protection Act 1998 (UK) (regarding disclosures of personal data required by law) was a centre-piece of the recent Supreme Court decision in *Rugby Football Union v Consolidated Information Services Limited (Formerly Viagogo) (In Liquidation)* [2012] UKSC 55, a case involving the making of a *Norwich Pharmacal* disclosure order of names and addresses of individuals allegedly involved in rugby match ticket scalping on the defendant's Viagogo website. Lord Kerr also referred in the case to the right to data protection in the EU Charter as relevant to the balancing process to be taken under section 35 (at [26]-[45]).

Further, the fact that Lord Leveson in his recent report on *The Culture, Practices and Ethics of the Press* (available at http://www.levesoninquiry.org.uk/?s=report) recommended reform of the UK Data Protection Act's section 32 journalism exception to limit its application to cases where "objectively, ... the likely interest in privacy resulting from the processing of the data is outweighed by the public interest in data protection" (rec 48), suggests that data protection might, if the reforms were made, take on a significant role in controlling the press's and more generally media's dealings with personal information.

The UK's Data Protection Act has been referred to from time to time as a possible additional source of protection in cases that are principally about privacy and/or confidentiality. Examples are *Campbell v Mirror Group Newspapers* [2004] 2 AC 457; *Murray v Express Newspapers* and *Tchenguiz v Imerman* [2010] EWCA Civ 908. The *Rugby Football Union* case can be seen in the same light – and indeed article 8 of the ECHR was also referred to in that judgment. In these cases it is still not clear what role data protection law might serve going beyond the protection already accorded by other doctrines. This is not just because of the Act's current rather uncertainly framed journalism exception (which in any event was not relevant in the *Tchenguiz* and *Rugby Football Union* cases). The Court of Appeal's decision in the early case of *Durant v Financial Services Authority* [2003] EWCA Civ 1746 that "personal data" in section 1 of the Act are essentially private biographical information has meant that, as the Court of Appeal said in *Tchenguiz*, "there is authority which supports the notion that that expression [ie personal data] should be given a narrow meaning" (at [96]). However, the Information Commissioner's Office takes a broader view, saying it is enough that data "'relate to' the identifiable living individual, whether in personal or family life, business or profession", following the European Article 29 Data Protection Working Party (see <http://www.ico.gov.uk/news/current_topics/what_is_personal_data.aspx>) – a position which seems closer to the *Rugby Football Union* case where names and addresses were treated as personal data (and see the discussion at [32]). Certainly, the draft Regulation

makes clear that for its purposes personal data will embrace "any information relating to a data subject" (see art 4).

Looking further afield, the European Directive's restrictions on cross-border transfers to countries that do not comply with its standards have helped to foster an international trend towards treating data protection as an important regulatory concept – building on the momentum of an earlier Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 as well as some OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 1980. As Graham Greenleaf's research shows, a large number of the world's jurisdictions have enacted or are in the process of enacting data protection laws ("Global Data Privacy Laws: 89 Countries, and Accelerating", Queen Mary University of London, School of Law Legal Studies Research Paper No 98/2012, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034 – in fact the number is now over 90). Moreover, many of these jurisdictions – including Canada, New Zealand and Australia – have taken steps to ensure that they not only have in place comprehensive data protection laws but that these laws meet minimum EU standards (albeit the process has not yet been altogether successful in Australia's case). Indeed, as Simon Chesterman observes with respect to Singapore's new data protection legislation, even in countries that have traditionally paid little attention to privacy, data protection law are being enacted to ensure that the countries can participate equally in the international trade environment ("After Privacy: The Rise of Facebook, the Fall of Wikileaks, and the Future of Data Protection", Working Paper, April 18, 2012, available at http://ssrn.com/abstract=2042144).

The US, of course, represents an important exception to the spread of EU-style data protection standards, with its negotiated "safe harbor" exception. And in general the US has long had a patchy record on data protection despite its Privacy Act 1974 (which is limited to federal government agencies). Some further substantive equivalence may be achieved if the "Consumer Privacy Bill of Rights" proposed in a White House paper of February 2012 (available at www.whitehouse.gov/sites/default/files/privacy-final.pdf) becomes US law, or even the rather weaker Federal Trade Commission recommendations in its report published in March 2012 (available at www.ftc.gov/os/2012/03/120326privacyreport.pdf) – including their provisions made about online tracking and profiling. And already, the Federal Trade Commissioner in recent years has actively used his powers under the Federal Trade Commission Act of 1914 to insist that internet companies are reasonably transparent in their treatment of personal data and substantial fines have been issued against *inter alia* Google and the social network site Path for non-compliance with these requirements – showing that although data protection may be a vilified concept in the US, consumer protection principles may in practice operate somewhat in the way of data protection.

But there is also much to suggest that privacy will continue to play an important role in all these jurisdictions. One reason undoubtedly is the long tradition of privacy. And it is not simply a history that began with Warren and Brandeis's important 1890 article. References to privacy can be found in ancient cases such as *Entick v Carrington* (1765) S C 19 How St Tri 1030 and *Prince Albert v Strange* (1849) 1 H & Tw 1, being cases still cited and relied on in modern discussions of privacy (as, for instance, with the lengthy discussion of *Entick v Carrington* in *US v Jones*). International instruments, such as the ECHR, the UN Declaration on Human Rights 1948 and the International Covenant on Civil and Political Rights 1966 give further support to the right to privacy as a traditional and venerable right. By contrast, the right to data protection is essentially a post-ECHR right – historically representing a response to new computer technologies of the 1960s and 1970s accompanied by fears about how these might be systematically used to monitor and control citizens.

Indeed, even now, the right to data protection does not have the same prestige-value as the right to privacy. It may have been characterised as a right of "informational self-determination", or "*Recht auf informationelle Selbstbestimmung*", in the German Census Act case of 1983 *(65 BVerfGE 1 at 43)*. But a central focus is the bureaucratic treatment of personal data; and principal concerns – when considered apart from privacy – are "equality and due process", as explained by Paul de Hert and Serge Gutwirth ("Data Protection in the Case Law of Strasbourg and Luxemburg" in Gutwirth *et al*, eds, *Reinventing Data Protection*, Dordrecht, Springer, 2009, 3 at 6). By contrast, Warren and Brandeis in their 1890 article could point persuasively to a right to privacy as essentially a right of personality reflecting deeply humanistic values. Similarly, in the more modern language of the ECtHR in the recent case of *Von Hannover v Germany (no 2)* 40660/08 [2012] ECHR 228 (February 7, 2012)

> *... the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings ([2012] ECHR 228 at [95]).*

In the end, this may explain why data protection is often intermingled with privacy, as if to give it an added expressive value. And, while it may be accepted that data can be "personal" yet not "private", the latter covering "aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity" (*Von Hannover v Germany (No 2)* [2012] ECHR 228 at [95]), a great range of personal data has been treated as private especially in recent cases. Fairly anodyne family activities were treated as *prima facie* within the right to private life in *Von Hannover v Germany (No 2)*, although

the countervailing interest in freedom of expression protected under article 10 ECHR prevailed in the circumstances of the case. Further, in *Copland v United Kingdom* [2007] ECHR 253 information in the plaintiff's emails was treated as private (without fine distinctions between aspects that were private and those that were not). And in the Ontario case of *Jones v Tsige* the plaintiff's bank records were also treated as generically private.

Similarly, names and addresses were considered not merely personal data in the *Rugby Football Union* case but private information as well – even if the interests on the side of data protection/privacy were not especially high when weighed against the "entirely worthy motive of the RFU in seeking to maintain the price of its tickets at a reasonable level", which could be seen both to promote the sport of rugby and to serve the interests of "members of the public who wish to avail of the chance to attend international matches"(at [45]). These cases may represent a more modern view of "private" information than *Durant v Financial Services Authority* where the FSA's records of Durant's complaint about Barclays Bank and the FSA's investigation of the complaint were considered too far removed from the plaintiff's identity to qualify as "private" (or "personal").

By the same token, the importance of data protection may also be bolstered by reference to confidentiality. Although confidentiality is not recognised as a human right, in the way of privacy, the idea of "trust and confidence" is an ancient and venerable concept in common law jurisdictions especially and its concerns have been treated as overlapping with those of data protection. Of course, privacy and confidentiality may also overlap. Indeed, in *Tchenguiz v Imerman*, where the plaintiff successfully claimed that his financial information held in a computer in an office shared with the first two defendants should be protected from their unauthorised access and use under a broad reading of the breach of confidence doctrine, the court said that this doctrine had to be seen as developing in tandem with the misuse of private information tort, stating that "consistency and coherence" are important given the "substantially increased focus on the right to privacy and confidentiality … over the past twenty years" ([2010] EWCA Civ 908 at [67]). At the same time, the court's reference to the potential application of the Data Protection Act to the defendants' conduct suggests that not only is the dividing line between a right to privacy and the right to data protection a thin one, becoming even thinner over time, so also is the line with breach of confidence – reinforcing the impression that traditional doctrines and concepts may be supplemented by newer ones from time to time but these can continue to develop in a harmonious fashion.

While the language of a "right to data protection" used in conjunction with a "right to privacy", or "private life", may imply the breakdown of a traditional distinction between a human right which is important to the individual's sense of self and a social right whose concern is with the workings of society, what we may ultimately get is a set of rights which combine both individual and social elements – reflecting, as Paul Schwartz says, the fact that

> *In the computer age, individual freedom cannot rest on a dream of being let alone by an ever-reduced government. Today, the safeguarding of liberty requires a legally structured pattern of access to and limitations on the use of personal information. The state has a critical role in ensuring that the processing of personal information is compatible with the individual's ability to participate in democratic self-rule. ("Privacy and participation: personal information and public sector regulation in the United States" (1995) 80 Iowa Law Review 557 at 618)*

But in practice the greatest change wrought by data protection standards may be around state and more generally public perceptions, of the best way to address systemic problems that go beyond the kinds of individual claims that privacy claimants have raised in their court cases in the past, with data protection and its institutional rubric including its data protection commissioners and offices seen as particularly well suited for these problems.

Megan Richardson
University of Melbourne.
This article was substantially written during a period of research leave at the Institute of Advanced Legal Studies in London between September and December 2012 and aspects were canvassed at a faculty seminar held at the Dickson Poon School of Law in October 2012 and a public seminar at the Institute for Advanced Legal Studies in December 2012, as well as in conversations with particular individuals. I am grateful for all the helpful advice received in the course of this very enriching period – as well as to friends and colleagues in Australia and New Zealand who provided further helpful comments and advice.