UNPRINCIPLED PRIVACY: WHY THE FOUNDATIONS OF DATA PROTECTION ARE FAILING US

SIMON DAVIES*

I INTRODUCTION

From time to time, the mechanisms employed to protect our fundamental rights must be reviewed and revamped – sometimes substantially so. For data protection (a particular aspect of the right to privacy), that moment is long overdue. The cherished mechanisms or principles that form the foundation of data protection are now more than 20 years old,[1] and their legal heritage is ancient. After so many years, battered and compromised by changing fortunes and changing times, stress fractures within the principles are now so prevalent that some areas of data protection are at risk of collapse. As a result, the nature and extent of privacy invasion has fundamentally eclipsed the capacity of law to provide limitations and redress.

Of course, there have been many occasions when the mechanisms intended to enforce data protection have in fact succeeded in protecting individuals, but it is doubtful that anyone in the profession of privacy advocacy can rationally argue that data protection, on balance, has worked as well as it might. In every country, privacy and, more specifically, data protection laws have failed at several fundamental levels to protect individuals. In Australia, limitations on the use of data have failed to prevent an extensive regime of public sector data matching;[2] in the same way, the collection limitation principle in United Kingdom ('UK') law has failed to prevent the breathtaking growth of visual surveillance in that

---

* Visiting Fellow, Department of Information Systems, the London School of Economics; Director, Privacy International (see Privacy International's website at <http://www.privacyinternational.org>).

1 See *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, ETS No 108 (entered into force 1 October 1985); Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980) (also at <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> at 22 May 2001).

2 See generally Graham Greenleaf (ed), *Privacy Law and Policy Reporter's Australian Privacy Guide* (1995) <http://austlii.edu.au/~graham/PLPR_australian_guide.html> at 25 June 2001, and various papers by Roger Clarke on data surveillance and information policy at <http://www.anu.edu.au/people/Roger.Clarke/DV/RogersDVBibl.html> at 25 June 2001.

country.[3] Even European data protection laws in general, arguably the most advanced in terms of recognising the importance of adequate data protection, have done little to prevent the spread of DNA testing, the use of identity cards, workplace surveillance, police powers, intrusion by tax authorities, Internet snooping and national security surveillance of civilian communications in the countries that comprise the European Union ('EU').

II THE PREVALENCE OF SURVEILLANCE

Taking surveillance as an example, public interest exemptions from data protection laws have resulted in wholesale violations of privacy. Governments and private sector organisations have moved – sometimes unimpeded – in recent years to incorporate surveillance into almost every aspect of our finances, communications and lifestyles. While acknowledging the importance of privacy as a fundamental right, data controllers argue that surveillance is necessary to maintain law and order and to create economic efficiency, and that privacy rights in general must remain subject to constraints of fiscal and public interest.[4] This argument is correct in principle, but frequently feeds on hypocrisy, deception and a total absence of any intellectual or analytical foundation, resulting in unreasonable extensions of surveillance.

When the Australian Government introduced the Australia Card Bill 1986 (Cth), it intended to create an unprecedented regime of surveillance on the basis of lurid and quite colourful claims that impending, rampant crime and spiralling administrative inefficiency warranted increased surveillance.[5] Yet at no time did the Attorney-General's Department (or any other authority) produce a threat analysis to justify such intrusion. After the defeat of the Australia Card proposal in 1987, the Government introduced legislation to implement both a national Tax File Number system and wholesale matching of government files.[6] Again, no comprehensive threat analysis was conducted and none was demanded, despite the passage of the *Privacy Act 1988* (Cth) ('*Privacy Act*') and the creation of a Federal Privacy Commissioner in early 1989. Under existing data protection legislation, such proposals are permitted under a variety of public interest exemptions without any requirements for a threat assessment, a sound justification, or even public discussion.

---

3 See EPIC and Privacy International, *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Developments* (2000) (also at <http://www.privacyinternational.org/survey/phr2000/countriesru.html#Heading15> at 22 May 2001).

4 See Simon Davies, 'The Spy in Your Refrigerator', *UNESCO Courier*, March 2001, 18. For a summary of key aspects of public interest see Simon Davies, *Taking Liberties in Confidence: A Report for the Nuffield Trust on the Implications of Clause 67 of the Health and Social Care Bill* (2001) <http://is.lse.ac.uk/privacy/Nuffield.htm> at 25 June 2001.

5 See Graham Greenleaf, 'The Australia Card: towards a national surveillance system' (1987) <http://austlii.edu.au/itlaw/articles/GGozcard.html> at 25 June 2001.

6 With respect to the latter, see *Data-matching Program (Assistance and Tax) Act 1990* (Cth).

In the dozen years since its implementation, the *Privacy Act* appears to have done little to stem the number of data collection schemes or the extent of privacy invasion generally in Australia. In fact, Australia in 2001 is a more hostile environment for privacy than at any time in its history. Increased levels of telecommunication interception, email snooping, genetic intrusion and visual surveillance provide a sobering insight into the true mechanics of privacy regulation. In the absence of restrictions on the creation of information collection schemes, the *Privacy Act* and the principles it contains can have only limited application on the fringes of intrusion.

If the principles of data protection were enforced across the information spectrum (without, for example, broad public interest exemptions), it is feasible that current legislation might offer substantial protection for individuals. However, there are three key factors that prevent this condition from occurring. First, governments generally tend to ensure that the most vital areas of their functioning are at least conditionally exempt from privacy law. Second, individuals – while consistently expressing anxiety about privacy invasion – are overwhelmed by the processes required to enforce protection of their privacy. Third, privacy and data protection regulators are frequently fatalistic, timid or under-resourced.

As a consequence of these conditions, communication and information infrastructures throughout the world are exhibiting a trend to 'surveillance by design', in which surveillance is established as a core design component of new systems. Global cooperation by law enforcement organisations, national security agencies and technical standards bodies ensures, for example, that all forms of new communication are 'wiretap friendly', and that new mobile technologies are capable of incorporating geographic tracking.[7] A global *Draft Convention on Cyber-crime* brokered by the Council of Europe intends to place such intrusions on a legal footing by harmonising and extending national laws to increase police powers, reduce the accountability of surveillance authorities, and limit the extent to which individuals can protect their privacy.[8] These initiatives are largely immune from data protection provisions, not so much because of the nature of data protection principles, but because of the *manner of their enforcement.*

If data protection principles were ruthlessly enforced, it is possible that they would limit, or even paralyse, such developments. However, in my opinion, the structure of much legislation, and the regulatory mechanisms in place, are actually incapable of providing the protection that they promise.

---

7 See the information on the Council of Europe's *Draft Convention on Cyber-crime*, ENFOPOL and Group of 8 activities at <http://www.privacyinternational.org/issues/cybercrime/> at 22 May 2001.

8 See Gus Hosein and David Banisar, *A Draft Commentary on the Council of Europe Cyber-crime Convention* (2000) <http://is.lse.ac.uk/staff/hosein/cybercrime/coe/coe_analysisver22.pdf> at 22 May 2001.

III THE CURRENT SYSTEM: ILLUSORY PROTECTION?

With a few notable exceptions, privacy regulators have remained mute about these shortcomings, choosing instead to pursue a low-key and uncontroversial style. The most charitable explanation for this approach is that privacy agencies worldwide are under-resourced, and must work 'within the system' to ensure their survival. A more sceptical interpretation is that some officials in control of these agencies regard the job as a career stepping stone, and have neither the motivation nor the skill to deal adequately with such a complex and fast moving issue. Whatever the explanation, the current mechanisms for enforcing data protection (and privacy protection in general) require serious, critical scrutiny. As David Flaherty (former Information and Privacy Commissioner of British Columbia) observed more than a decade ago, our nations have become surveillance societies, and we must ask ourselves whether existing data protection laws and the agencies which police them offer only the illusion of protection.[9]

Even if everyone (including governments and law enforcement agencies) were to agree that the principles of data protection should be immutable and unchanging, the application or enforcement of those principles in the real world would need to be subjected to rigorous and dispassionate criticism. That people should, for example, be given the legal right to gain access to their data is beyond question. The issue, surely, is whether in 2001 the means of achieving this right are adequate (or, indeed, whether they have any practical value whatever).

Like many privacy advocates, I often find myself instinctively defending entrenched conventions of data protection. 'Functional separation', 'collection limitation', 'fair use'[10] – these are concepts that underpin data protection, and which must be rigorously defended and promoted. And yet such mechanisms have clearly failed to prevent the most significant and far-reaching abuses of privacy. In the face of such criticism, privacy officials (and their biographers) tend to promote success stories, adopting a 'celebratory tone'.[11] While this is understandable, all professions are constantly at risk of sacrificing their responsibilities on the altar of pragmatism, and the area of privacy protection is no exception. Privacy officials all too often abuse the trust placed in them by dodging controversy in an effort to preserve their fiefdoms. As a consequence, governments frequently succeed in using data protection law as a thinly veiled mandate for surveillance.

These are not radical or extreme views. Once a fundamental right has been agreed upon, and once basic means of protection have been established, it is the

---

9 A comprehensive analysis of the activities of data protection regulators can be found in David Flaherty, *Protecting Privacy in Surveillance Societies* (1989).

10 These principles refer to (in order): (a) ensuring that each information system is operated independently of other systems, and that data is not transferred between systems; (b) ensuring that the collection of data is kept to the minimum amount necessary to undertake the task related to the data; and (c) ensuring that the processing of data conforms to a set of principles safeguarding individuals' privacy rights.

11 Flaherty, above n 9, xiv.

transgressors who become radical. The rigorous protection of rights is a *conservative* notion, yet this reality is conveniently inverted by government and the private sector alike.

Perhaps for fear of being branded radical, privacy regulators are often reluctant to rigorously enforce the core principles. Given the parlous state of privacy across the world, they should be more attentive to this responsibility. In the modern age for example, notification and consent (as mechanisms of privacy protection) have largely become fraudulent notions. In theory, the collection and use of information about individuals is predicated on the idea that people should be informed as to the proposed use of their information, and that they should generally be able to withhold consent. In reality, these rights are impractical, unknown and ignored; consent has become a mechanism for guaranteeing continuous data flows, rather than a means to ensure the protection of individual rights.

The most telling evidence of this failure to enforce the basic means of privacy protection was recently produced by Consumers International, a London based federation of 263 consumer organisations. In January 2001, Consumers International released the findings of a study of the privacy practices of Internet sites worldwide, which found that the vast majority of sites gave users no choice about being on the site's own mailing list or having their name passed on to affiliates or third parties.[12] Despite EU action in this area, sites within the EU proved to be no better at informing users about how they used their data than sites based in the United States ('US'). Indeed, some of the best privacy policies were found on US sites.

Consumers International concluded that 'too many companies collect a lot of unnecessary, very personal information about their customers – and because of inadequate implementation of existing government measures people don't have control over their data'.[13] This widespread neglect of good privacy practice is even more worrying given the speed at which electronic technologies for the collection of data are developing. The implementation issue becomes crucial: for example, if companies in Europe (where there is arguably the greatest level of privacy regulation) can fulfil the letter of the law by providing customers with consent forms containing 'opt in or opt out' boxes that only require a tick, they can hardly be expected to entirely fulfil (or seek to fulfil) the fundamental European expectation of 'informed consent'. This standard can therefore only become meaningful through general public education, a process that has barely commenced.

---

12 Consumers International, *Privacy@net: An international comparative study of consumer privacy on the internet* (2001) <http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf> at 22 May 2001.

13 Consumers International, *Consumer Privacy Threatened on the Net: US and EU Websites Fall Short of the International Standards on Privacy*, Press Release (25 January 2001) (also at <http://www.consumersinternational.org/news/pressreleases/privacy250101.html> at 22 May 2001).

IV THE PROTECTION OF PRIVACY AS A PUBLIC INTEREST IN ITSELF

Is it possible to establish mechanisms to ensure that people are informed about the existence and use of their data? Most techniques employed to date have failed. For example, the *Personal Information Digest*, published regularly by the Australian Federal Privacy Commissioner, pursues the quite laudable aim of telling people which Federal Government organisations hold particular categories of data.[14] The most recent edition has grown to an impressive 320 000 words, but in reality the *Digest* is of practical benefit to only a very small number of legal professionals and campaigners who know it exists and who can unravel its complexity. The work and expense involved in producing the volume has supplanted the more vital task of vetting the information supplied to the Commissioner for accuracy and completeness.[15]

The approach adopted by the UK Data Protection Commissioner, which involves the compilation of a register of data controllers,[16] is of similarly limited value to consumers, and appears now to be more frequently used as a commercial intelligence-gathering tool. The 'watchdog', non-governmental organisation Privacy International has estimated that personal data on the average resident of the developed world is located on at least 400 key databases, and that gaining access to this data – even if the existence of such databases was readily known to the individual – would consume more than eight working weeks in preparation, administration and analysis. Since only a fraction of the data holdings are derived directly from the individual, it is highly unlikely that an individual could find out which particular organisations are holding data on them.

Yet these failures should not create a motivation to eliminate the current laws but to strengthen them. The data protection principles that form the foundations of modern privacy law (for example, collection limitation, limitation on disclosure and access to personal data) are largely sound and relevant, but they have been corrupted and compromised through timidity and neglect. In Australia, perhaps more than in most developed countries, recent experience has established that action must be taken to substantially limit the collection of data even where authorities provide a thorough and genuine justification. The preservation of privacy should not be viewed as an encumbrance that can be diluted through 'public interest' exemptions, but as a public interest *in itself*. Further, consent should no longer be regarded as the key mechanism for protecting personal information. And, perhaps most importantly, privacy regulators should vigorously enforce both the spirit and the letter of the privacy laws. If they fail to do so – as many have – the public should rightly see them as part of the problem, rather than part of the solution.

---

14 See, eg, Office of the Federal Privacy Commissioner, *The 2000 Commonwealth Personal Information Digest* (2000) (also at <http://www.privacy.gov.au/publications/pg1pubs.html#8.1.1> at 22 May 2001).

15 The Preface to the *Digest* states that the Privacy Commissioner is unable to verify the accuracy or completeness of the information.

16 All data systems in the UK must be individually registered with the Data Commissioner.