THE PLACE OF PRIVACY IN DATA PROTECTION LAW

LEE A BYGRAVE*

I INTRODUCTION

The concept of privacy has rarely featured explicitly in Australian law and legal discourse. The modest prominence it currently enjoys is due mainly to the enactment and gradual extension in coverage of data protection legislation, most notably in the form of the *Privacy Act 1988* (Cth). This is not to say that the *interest* in privacy remains unprotected by other elements of the law in Australia, but that the protection afforded by these elements tends to omit express reference to privacy.

In this article, I examine the relationship between the concept of privacy and data protection laws.[1] In particular, I question the almost universal consensus that data protection legislation exists largely to protect the 'privacy' of individual persons. This depiction of the rationale of data protection legislation tends to be accepted without serious analysis of its veracity. It is my contention that it is somewhat flawed.

II THE FAILURE TO DEFINE PRIVACY IN DATA PROTECTION LAW

It is difficult to disagree with the proposition that data protection laws are, to some extent at least, concerned with safeguarding personal privacy. This concern is expressly manifest in the titles and opening provisions of many data protection laws. Yet despite its high profile in data protection law and discourse in

* BA (Hons), LLB (Hons) (ANU); Dr juris/ LLD (Oslo); Senior Research Fellow, Norwegian Research Centre for Computers and Law, University of Oslo; Barrister of the Supreme Court of New South Wales.

1 Although this will be obvious for many readers, 'data protection law' denotes a set of rules which specifically regulate all or most stages in the processing of 'personal information' – ie, information relating to, and permitting identification of, individual persons (and sometimes organisations) – and which embody the bulk of principles laid down in recognised data protection instruments, such as the Organisation for Economic Co-operation and Development *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980). For an overview of these principles see Lee A Bygrave, 'An international data protection stocktake @ 2000: Core principles of data protection' Pt 2 (2001) 7 *Privacy Law and Policy Reporter* 169.

countries such as Australia, the concept of privacy remains nebulous. Indeed, privacy is never directly defined in those data protection laws that employ the term. The laws which come closest to defining the term only provide definitions of what amounts to a *breach* of privacy for the purposes of each Act.[2] Hence, the meaning of privacy for the purposes of data protection law must be sought partly in the substance of the principles laid down in the laws themselves, partly in the way those principles have been applied, and partly in general, societal notions of what privacy is.

The failure to define privacy in data protection laws undoubtedly reflects the notorious difficulties that have plagued attempts to give privacy a precise, analytically serviceable and generally accepted meaning. At the same time, this failure is not necessarily a weakness in data protection laws: it can provide room for flexibility in their implementation. Further, the apparently inherent vagueness of the privacy concept enables it (and thereby data protection law) to assimilate and address a range of fears related to increasingly intrusive data-processing practices. Indeed, this characteristic undoubtedly helps to explain the protracted prominence of the privacy concept in data protection discourse. Moreover, data protection advocates have probably found it useful to adopt, in the words of Freund, 'a large concept in order to offset an equally large rhetorical counter-claim: freedom of inquiry, the right to know, liberty of the press' and so on.[3]

Nevertheless, the failure to define privacy in data protection laws has a cost in so far as it detracts from the capacity of those laws for prescriptive guidance. A further cost is that it perpetuates the vulnerability of the privacy concept to the criticisms that it is incapable of definition, has no independent, coherent meaning and should be subsumed by other concepts.[4] This cost is difficult to tolerate for persons (such as myself) who see privacy as denoting a distinct value that is not adequately delineated by other notions, and who believe, accordingly, that normative discourse would be impoverished should this concept fall into disuse.

Notwithstanding the above remarks, the concept of privacy remains open to numerous definitions and an extensive debate has raged over which definition is the most correct.[5] Before examining the various definitions, it is important to note that such a debate carries with it various dangers, including underplaying the multidimensional character of privacy and overlooking the fact that law and policy do not always need to operate with precise definitions of values. Furthermore, the debate is difficult to resolve conclusively because it rests to a considerable extent on intuitive assessments of how privacy should be commonly understood.

---

2 See, eg, *Privacy Act 1988* (Cth) ss 13, 13A.

3 Paul Abraham Freund, 'Privacy: One Concept or Many' in J Roland Pennock and John W Chapman (eds), *Privacy: Nomos XIII* (1971) 182, 193.

4 Such criticisms are advanced in, eg, Judith Jarvis Thomson, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295.

5 For an overview of the lines of debate, see generally Julie C Inness, *Privacy, Intimacy, and Isolation* (1992) ch 2.

III THE MEANING(S) OF PRIVACY IN DATA PROTECTION LAW

Analysis of the literature on privacy reveals four major ways of defining the concept. Amongst the most popular definitions of privacy in data protection discourse are those framed in terms of 'information control'.[6] The most influential of such definitions is the following, given by Alan Westin: 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[7] The popularity of these sorts of definitions in data protection discourse is not surprising, as they appear directly applicable to the issues raised by the data-processing practices of organisations. They also harmonise fairly well with, and build upon, many of the basic rules of data protection law, particularly those rules that enable persons to participate in, and influence, the processing of information about them.[8] Furthermore, a control-based definition of privacy arguably lends the concept of privacy considerable normative force, as it allows privacy advocates to tap into the dynamic ethical undercurrent associated with the ideal of self-determination.

At the same time, it is important to note that data protection laws rarely give persons an absolute right to dispense with data about themselves as they see fit. Thus, the laws are better viewed as manifestations of an interest in informational *co*-determination as opposed to self-determination. Furthermore, conflating privacy with control might serve to rob privacy of its conceptual uniqueness, and thereby detract from the force of privacy advocacy in the long run. Witness, for instance, the considerable criticism of United States ('US') case law on the constitutional right to privacy, in which that right has been used to address issues that essentially concern autonomy.[9]

A further two groups of definitions characterise privacy in terms of non-interference and limited accessibility respectively. The non-interference definition gained prominence largely in the wake of the famous *Harvard Law Review* article by Samuel Warren and Louis Brandeis, who argued that the right to privacy in Anglo-American common law is part and parcel of a right 'to be let alone'.[10] A leading example of the characterisation of privacy as a condition of limited accessibility is Ruth Gavison's definition. According to Gavison, this

---

6 See, eg, the definitions advanced in: *Private Word – News from the Office of the [New Zealand] Privacy Commissioner* No 4, April 1996, 6; Ragnar Dag Blekeli, 'Framework for the Analysis of Privacy and Information Systems' in Jon Bing and Knut S Selmer (eds), *A Decade of Computers and Law* (1980) 21, 24; United Kingdom, Committee on Data Processing, *Report of the Committee on Data Protection* (Cmnd 7341, 1978) 10, [2.04]; Stefano Rodotà, 'Protecting Informational Privacy: Trends and Problems' in Willem F Korthals Altes *et al* (eds), *Information Law Towards the 21st Century* (1992) 261.

7 Alan F Westin, *Privacy and Freedom* (1970) 7.

8 See, eg, *Privacy Act 1988* (Cth) sch 3, National Privacy Principles 1.3, 2.1(b) and 6.

9 See, eg, Raymond Wacks, 'The Poverty of Privacy' (1980) 96 *Law Quarterly Review* 73, 78 ff; H Gross, 'Privacy and Autonomy' in J Roland Pennock and John W Chapman (eds), *Privacy: Nomos XIII* (1971) 169, 180-1.

10 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890-91) 4 *Harvard Law Review* 193, 195.

condition consists of three elements: 'secrecy' ('the extent to which we are known to others'); 'solitude' ('the extent to which others have physical access to us'); and 'anonymity' ('the extent to which we are the subject of others' attention').[11]

Concerns about non-interference and limited accessibility can be found in numerous data protection provisions, especially those restricting the amount of personal information that can be gathered, the secondary uses to which the information can be put and the classes of persons and organisations to which the information can be disclosed.[12] Implementation of these provisions restricts the ability of people and organisations to gain access to information about others. It can also decrease the chance of persons being asked to supply information on themselves and can thereby decrease the extent to which they suffer interference or attention from information gatherers. The same can be said for provisions requiring that measures be taken to safeguard or improve information quality.[13] Implementation of such provisions lessens the risk of a decision being made about a person on the basis of inaccurate or irrelevant information. This, in turn, lessens the risk of the decision maker then taking, say, unwarranted investigative action which interferes with or disturbs that person.

The fourth class of definitions relates privacy exclusively to those aspects of persons' lives that are 'intimate' or 'sensitive'. Julie Inness, for example, defines privacy as 'the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions'.[14] According to this view of privacy, not every disclosure of information about a person will amount to a loss of privacy; there will only be a loss when 'sensitive' or 'intimate' personal information is disclosed.[15] This conception of privacy is relatively unpopular in data protection discourse mainly because intimacy-oriented definitions of privacy are unable to anticipate and capture the process by which detailed personal profiles of individuals are created through combining disparate pieces of ostensibly innocuous information. By 'innocuous' information I mean information that, on its own, is not sensitive or intimate. The aggregation of such information currently constitutes one of the major methods of creating detailed and intimate personal profiles. As administrative systems in both the public and private sectors become increasingly integrated, such aggregation is likely to occur on an even larger scale. Any conception of privacy which does not capture or reflect this process is of relatively little utility for present and future appreciation of data protection issues.

Accordingly, few direct manifestations of intimacy-oriented conceptions of privacy are to be found in the provisions of data protection laws. The ambit of

---

11 Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 428-36. In my opinion, this conception of privacy comes closest to capturing the core of the concept at the same time as it does relatively large justice to the concept's multidimensionality.

12 See, eg, *Privacy Act 1988* (Cth) sch 3, National Privacy Principles 1.1, 1.2, 2.1, 4 and 8.

13 See, eg, *Privacy Act 1988* (Cth) sch 3, National Privacy Principle 3.

14 Inness, above n 5, 140.

15 Ibid 58 ff.

such laws is generally not limited to information of a particular, predefined quality about persons.[16] Nevertheless, direct manifestations of intimacy-oriented conceptions of privacy do occur in the provisions that place extra restrictions on the processing of certain categories of especially sensitive, personal data.[17]

IV THE RELATIVE IMPORTANCE OF PRIVACY IN DATA PROTECTION LAWS

Ample grounds exist then for the view that privacy has a central place in data protection law, at least if privacy is defined in terms of information control, non-interference or limited accessibility. Nevertheless, it would be wrong to characterise data protection law as *solely* concerned with privacy for several reasons.

First, the protection of privacy serves a large range of other values and interests, the safeguarding of which must accordingly form part of the rationale and agenda of data protection law. Important examples of such values are personal autonomy, integrity and dignity. These values can be summed up as being largely concerned with 'achieving individual goals of self-realization'.[18] At the same time, such values, along with privacy, are not only relevant to the well-being of individual persons – they also have a broader societal significance. Their protection helps to constitute a society infused with civility, stability, pluralism and democracy.[19] Realisation of these general societal values must, therefore, also be recognised and treated as an integral part of law and policy on data protection.

Secondly, data protection instruments are expressly concerned with setting standards for the quality of personal information. While adequate information quality can serve to secure the privacy of individuals, it breaks down into a multiplicity of interests (including concern for, inter alia, the validity, integrity, availability, relevance and completeness of data) that have little *direct* connection to privacy-related values.[20]

Thirdly, data protection laws are also concerned with ensuring that individuals and organisations are able to process information about others for various legitimate ends. Indeed, data protection laws generally do not attempt to assail most established systems of administration, organisation and control of information; rather, they tend to seek to manage these systems in a manner that

16 Hence Inness, who champions an intimacy-oriented definition of privacy, claims it is misconceived to characterise data protection laws as concerned with privacy. In her view, it is better to characterise such laws as protecting 'secrecy': ibid 60-1.

17 See, eg, *Privacy Act 1988* (Cth) sch 3, National Privacy Principle 10.

18 Westin, above n 7, 39.

19 See Lee A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (1999) [7.2.2], [7.2.5].

20 For an elaboration of these interests, see ibid [7.2.5].

makes them more palatable to (and, hence, legitimate from the perspective of) the general populace.[21]

Extending this point, it can be argued that data protection laws have much the same aim and function that policies of 'sustainable development' have in the field of environmental protection. Data protection laws seek to safeguard the privacy and related interests of data subjects at the same time as they seek to secure the legitimate interests of data controllers in processing personal data just as policies of 'sustainable development' seek to preserve the natural environment at the same time as they allow for economic growth. Both policy concepts promote a belief that the potential for conflict between these respective sets of interests can be significantly reduced through appropriate management strategies. Concomitantly, both policy concepts can be used to create an impression that the interests of data subjects and the natural environment are adequately secured, even when their respective counter-interests are also secured.

V CONCLUSIONS

Thus, while privacy does occupy a central place in data protection law, characterisation of data protection law as solely or even essentially concerned with safeguarding privacy is misleading. Data protection laws serve a multiplicity of interests, which in some cases extend well beyond traditional conceptualisations of privacy. Thus, the consensus identified at the beginning of this article tends to underplay the complexity of data protection legislation.

This consensus also runs the risk of underplaying the fact that the focus and agenda of data protection laws are constantly developing. These changes are sometimes reflected in the text of the laws themselves,[22] and sometimes in the range of decisions and actions taken by data protection authorities, especially when the latter are given broad discretionary powers.[23]

Finally, the view that data protection is essentially privacy protection runs the risk of obscuring the fact that data protection laws benefit not only individuals *qua* individuals but society as a whole. The insight that privacy safeguards have broad societal benefits is not something that can be taken for granted. Much of the discourse on privacy and privacy rights has tended to focus only on the benefits these have for individuals *qua* individuals, and therefore to see such rights as essentially in conflict with the needs of 'society'.[24] This has been accompanied by a considerable literature seeking to highlight various ways in

---

21 See James Rule *et al*, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (1980) 71 ff.

22 See, eg, 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, art 15 (which deals innovatively with certain types of fully automated decision-making).

23 For examples, see Bygrave, above n 19, [7.2.4].

24 See Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (1995) chh 2, 8. Regan's analysis deals primarily with US discourse but is also valid for privacy discourse in other countries, such as Australia.

which privacy rights detract from the common good.[25] These tendencies can have the unfortunate consequence of leading to a skewed appreciation of the societal benefits of privacy rights, thus hampering advocacy for strong(er) data protection laws.

25 Typical criticisms of privacy rights are that they entrench social hierarchies, promote insularity and intolerance, and permit deception and hypocrisy to flourish. See, eg, Koen Raes, 'The Privacy of Technology and the Technology of Privacy: The Rise of Privatism and the Deprivation of Public Culture' in András Sajó and Ferenc B Petrik (eds), *High-Technology and Law: A Critical Approach* (1989) 73; Richard A Posner, 'The Right to Privacy' (1978) 12 *Georgia Law Review* 393. While some of these criticisms have a limited validity, they are frequently advanced in an overly blunt and simplistic manner. Concomitantly, they often fail to take adequately into account the fact that privacy rights co-exist with, and are balanced and modified by, a range of other rules, and that it is the function of privacy rights in the overall scheme of a legal system which is crucial to any assessment of their effects.