AN EXPLORATION OF THE CONCEPTUAL BASIS OF PRIVACY AND THE IMPLICATIONS FOR THE FUTURE OF AUSTRALIAN PRIVACY LAW

DAVID LINDSAY*

[Recent years have seen significant developments in the protection of privacy at general law in common law jurisdictions, including the United Kingdom and New Zealand. Although the general law protection of privacy in Australia is uncertain, there has been a proliferation of information privacy laws at both federal and state levels. This article contends that the future development of privacy law in Australia should be based upon a rigorous analysis of the complex concept of privacy. As a first step in this analysis, the article reviews the main approaches that have been taken to the concept of privacy, distinguishing deontological from consequentialist approaches. The article claims that these two approaches are related, in general terms, to the two main Western legal approaches to privacy protection: the European 'rights-based' and the American 'market-based' approaches. Drawing upon Foucauldian analysis, the article claims that privacy law can be understood within the context of ongoing social processes of normalisation and rationalisation. As such, our understanding of privacy law can be assisted by relating it to an important Western political tradition — including thinkers such as Weber, Heidegger, Foucault and Habermas — that is ambivalent about market-based and bureaucratic rationalisation. Assuming this to be the case, both 'rights-based' and 'market-based' approaches can be seen as reinforcing social rationalisation. Within an overwhelmingly consequentialist society such as Australia, however, a 'rights-based' approach to privacy law may be preferred as a way of resisting global pressures for social rationalisation, and as a form of protection for pluralistic social identities.]

CONTENTS

* BA, LLB (Syd), LLM (Melb); Senior Lecturer, Faculty of Law, Monash University. This article was written with research funding from an Australian Research Council grant, 'Establishing an Optimal Regime for the Protection of Online Privacy'. The author would like to thank the Chief Investigators for the project, Professor Sam Ricketson and Associate Professor Megan Richardson from the Law School, The University of Melbourne, and Ms Lesley Hitchens from the Faculty of Law, The University of New South Wales, for their advice and assistance with this work. The author would also like to acknowledge the helpful comments of the referees for this article. All errors are, of course, my own.

I INTRODUCTION

Australian privacy law has reached a point where it would be desirable for future developments to be based on a deeper analysis of the concept of privacy and its role within Australian society. Unless this analysis is undertaken, it is unlikely that the future development of privacy law in Australia will be satisfactory or principled. It is imperative for the analysis to be undertaken because Australian privacy law is assuming increasing social and economic significance while, at the same time, undergoing fundamental transformation.

The challenges facing the protection of privacy at general law in Australia were foreshadowed by Gleeson CJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*, who maintained that '[t]he law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy.'[1]

Since these comments, there have been significant developments in the protection of privacy at general law in New Zealand and in the United Kingdom, both expressly influenced by rights-based jurisprudence. In *Campbell v MGN Ltd*,[2] the House of Lords continued and confirmed the preference of English courts to protect privacy by extending the action for breach of confidence, while incorporating arts 8 (the right to privacy) and 10 (the right to freedom of expression) of the *European Convention for the Protection of Human Rights and Fundamental Freedoms*[3] within the parameters of the established action for breach of confi-

[1] (2001) 208 CLR 199, 225.
[2] [2004] 2 AC 457.
[3] Opened for signature 4 November 1950, 213 UNTS 222 (entered into force 3 September 1953).

dence. In *Hosking v Runting*,[4] on the other hand, the majority of the New Zealand Court of Appeal definitively recognised a tort of public disclosure of private facts. In doing so, Gault P and Blanchard J specifically stated that:

> The emergence internationally of concern for the protection of human rights and of individual consumers provides examples reflecting the shift in emphasis from the traditional approach to tort liability (liability for reprehensible conduct) *to the protection of identified rights*.[5]

If the question of the protection of privacy under the general law comes before the Australian High Court, the relative merits of the approaches adopted by courts in the United Kingdom and in New Zealand should be assessed.[6] In doing so, the eventual shape of the law may be influenced by the traditional Australian reticence towards 'rights'.

The emergence of a higher level of protection of privacy at general law should not be viewed in isolation from legislative developments conferring greater protection on privacy. In fact, the most significant legal development in the protection of privacy under Australian law has been the proliferation of information privacy, or 'data protection', laws.[7] Despite these developments, the conceptual underpinnings of Australia's information privacy laws have not been clearly enunciated.

The practical consequences of this failure cannot be underestimated. Under European Union ('EU') data protection law, a Working Party has been established to assess the 'adequacy' of the level of protection given by non-EU countries to personal data which may be transmitted by EU citizens.[8] In January 2001, the Working Party published an Opinion which expressed concerns regarding the 'adequacy' of the Australian federal private sector regime.[9] A greater appreciation of the extent to which European data protection law is based on a concept of privacy that draws upon Continental human rights traditions is essential to understanding the tensions between the EU and the Australian government on this issue. Defending policy differences with the EU will be difficult as long as the conceptual foundations of Australian information privacy laws are poorly understood and articulated.

4 [2005] 1 NZLR 1.

5 Ibid 5 (emphasis added).

6 There are potentially important differences between a privacy tort and the extended action for breach of confidence, including implications for defences and remedies.

7 See, eg, *Privacy Amendment (Private Sector) Act 2000* (Cth); *Privacy and Personal Information Protection Act 1998* (NSW); *Information Act 2002* (NT); *Information Privacy Act 2000* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT); *Health Records and Information Privacy Act 2002* (NSW); *Personal Information Protection Act 2004* (Tas); *Health Records Act 2001* (Vic). See also recommendations for introducing information privacy legislation in Western Australia: Office of the Attorney-General for Western Australia, *Privacy Legislation for Western Australia Policy Research Paper* (2003).

8 The Working Party on the Protection of Individuals with regard to the Processing of Personal Data ('Working Party') was established by art 29 of *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 281/31, 48.

9 Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, adopted on 26 January 2001, Doc No 5095/00/EN WP40 final.

This article contends that the uncertain development of the protection of privacy at general law, and the difficulties confronting Australian information privacy laws, can be traced to a common source: an inadequate analysis and articulation of an Australian approach to the concept of privacy.

In further exploring the role of the concept of privacy under Australian law, the article makes a number of claims. First, the central connection between the concept of privacy and modern Western political and legal traditions is explained. In particular, privacy is related to two linked processes that are at the heart of modern Western practices of social ordering. Privacy is, first of all, central to the creation of forms of subjectivity marked by strong individual identities. In other words, the creation of individual subjects, conventionally defined in opposition to others, depends upon particular forms of withholding and disclosure of aspects of the self.[10] In addition, the concept of privacy is related to a major strand of modern Western political and legal thought, one that is characterised by fundamental disquiet with the perceived excesses of political and administrative rationality.

Secondly, this article contends that there is a fundamental divergence between the two main approaches to privacy within the Western legal tradition, which can be conveniently labelled the 'European approach' and the 'American approach'. It is important to understand that there are entrenched and growing differences in the underlying assumptions and essential orientations of contemporary European and American legal traditions. The approach taken to the protection of privacy within the Australian legal system must necessarily refer to these two approaches, which should now be seen as rivals, despite their common historical roots in the Enlightenment.

Thirdly, this article links the divergence in approaches to privacy to an unresolved tension within the Western tradition: whether the legal protection of values, such as privacy, is subservient to instrumental goals, such as economic rationality or efficiency, or whether it should be directed at promoting the non-instrumental values of human dignity and individual autonomy. In other words, should privacy law protect individuals as 'empirical consumers' or as 'ideal citizens'? The suggested answer is that the approach adopted by the law should depend upon whether a consequentialist or deontological approach is taken to the concept of privacy.

This article has six main parts. The first part discusses conceptual difficulties with the concept of privacy and proposes a new Foucault-influenced approach, in which 'privacy' should be understood in the context of ubiquitous micro-struggles over identity within totalising social practices. The second part examines the main conceptual justifications for privacy laws, distinguishing deontological from consequentialist accounts, and attempts to relate the traditional justifications to the new understanding of privacy. The third part describes the historical origins of the most important 'new' form of privacy law: information privacy or data protection laws. It explains the different social and political sources of American information privacy laws on the one hand, and European

[10] See, eg, Thomas Nagel, *Concealment and Exposure* (2002).

data protection laws on the other. The fourth part deals with the traditional justifications for information privacy laws, again distinguishing deontological from consequentialist accounts, and further explains how these justifications relate to arguments for privacy protection more generally. The fifth part explains the increasing divergence between American and European approaches to data protection, and relates the differences to the distinction between consequentialist and deontological accounts of information privacy. The sixth part summarises the issues at stake in the conflict between European and American approaches to information privacy, and explains the choices facing Australian privacy law. The conclusion suggests a preferred approach to shaping privacy laws in Australia, drawing upon the proposed new understanding of the concept of privacy.

II THE CONCEPT OF PRIVACY

The concept of privacy occupies an especially difficult position in Western legal and political discourse. It is an 'elusive' concept that is difficult to define in any satisfactory manner.[11] As long ago as 1873, Sir James Fitzjames Stephen concluded that '[t]o define the province of privacy distinctly is impossible'.[12] Since then, a daunting literature has developed, which appears to have approached privacy from every possible theoretical and political position.[13] In fact, the most notable feature of this literature has been an almost complete absence of agreement concerning both the definition of privacy and the values said to be promoted by the legal protection of privacy.[14]

For a concept that has become central to contemporary political concerns, it is surprising that philosophical and legal analysis of privacy as a distinct concept did not commence in earnest, at least in the English-speaking world, until the late 1960s.[15] The formidable, predominantly American, literature which then emerged[16] can be directly ascribed to three developments. First, in the United

[11] In 1983, the Australian Law Reform Commission stated that '[t]he very term "privacy" is one fraught with difficulty. The concept is an elusive one. There have been numerous attempts to define it, and none has been altogether satisfactory': Australian Law Reform Commission, *Privacy*, Report No 22 (1983) [19] (citations omitted).

[12] Sir James Fitzjames Stephen, *Liberty, Equality, Fraternity* (first published 1873, 1967 ed) 160. Stephen went on, however, to propose an impossibly broad 'description' of privacy as '[c]onduct which can be described as indecent': at 160.

[13] As David Flaherty explains in relation to the task of defining privacy, 'philosophers continue to bemuse themselves with this important activity, it would appear, while individual authors parade their ingenuity with increasingly obscure, and obscuring, definitions': David Flaherty, 'Controlling Surveillance: Can Privacy Protection Be Made Effective?' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997) 167, 171.

[14] As Robert Gellman has remarked, '[l]awyers, 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': Robert Gellman, 'Does Privacy Law Work?' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997) 193, 193.

[15] According to Ferdinand Schoeman, 'there was no major philosophical discussion of the value of privacy until the late 1960s': Ferdinand Schoeman, 'Privacy: Philosophical Dimensions of the Literature' in Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 1, 1.

[16] Some of the most significant philosophical and legal articles dealing with the concept of privacy are found in the following collections: J Roland Pennock and John Chapman (eds), *Privacy*

States the 1950s and 1960s saw a considerable increase in surveillance technologies and practices, including electronic surveillance of individuals by government agencies such as the Federal Bureau of Investigation.[17] The legal reaction to the increased use of surveillance culminated in the 1967 Supreme Court decision in *Katz v United States*,[18] which held that the Fourth Amendment protection against unreasonable searches and seizures extended to protect telecommunications from interception without a warrant. Secondly, there were underlying concerns arising from the proposed use of computerised systems by governments for collecting and processing personal information, which gave rise to modern information privacy law.[19] Thirdly, there was the recognition in the seminal Supreme Court decision of *Griswold v Connecticut* of a new form of constitutional protection of privacy as an unenumerated right under United States law.[20] The Court's decision in *Griswold* gave rise to a controversial jurisprudence concerning a sphere of individual decision-making immune from state proscription.[21]

The troubled history of the concept of privacy in Western philosophical and legal traditions poses two important related questions that must be addressed before progress can be made in examining the concept. First, why has defining the concept of privacy proven to be intractable or, at least, why has analysis of the concept been much more difficult than comparable analyses of other complex social and political concepts, including liberty and freedom of expression? Secondly, why have particular Western legal systems accorded legal recognition to privacy at particular points in history, albeit that the precise forms of legal protection have been less than coherent?

A *Difficulties in Defining Privacy*

There are a number of possible explanations for the dissension and confusion surrounding the concept of privacy. To begin with, there are well-known difficulties associated with defining all complex social and political concepts. Many attempts at defining privacy have been unsophisticated. For example, most definitions proposed by theorists have attempted to distinguish privacy from related concepts, such as secrecy or autonomy, by stating necessary and suffi-

(1971); John Young (ed), *Privacy* (1978); Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984); Raymond Wacks (ed), *Privacy* (1993).

17 See Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (1998); Ken Gormley, 'One Hundred Years of Privacy' [1992] *Wisconsin Law Review* 1335, 1363–7; Daniel Solove, 'The Origins and Growth of Information Privacy Law' (2003) 748 *PLI/Pat* 29, 53–6.

18 389 US 347 (1967).

19 As David Banisar and Simon Davies point out, '[i]nterest in the right of privacy increased in the 1960s and 1970s with the advent of IT': David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18 *John Marshall Journal of Computer and Information Law* 1, 10.

20 381 US 479 (1965) ('*Griswold*'). As Judith DeCew has explained, '[m]uch of the discussion of privacy has evolved from a constellation of legal judgments. Philosophers then entered the debate, attempting to illuminate just what a right to privacy can and should mean': Judith DeCew, 'The Scope of Privacy in Law and Ethics' (1986) 5 *Law and Philosophy* 145, 146.

21 See, most recently, the decision of the United States Supreme Court in *Lawrence v Texas*, 539 US 558 (2003).

cient conditions that set privacy apart.[22] In other words, there have been attempts to attribute an essential meaning to the concept. In the 20th century, however, essentialism was rejected as a useful means of defining words or concepts.[23]

A further difficulty with defining key social and political terms is the extent to which concepts such as privacy are thoroughly value-laden, leading to suggestions that it is impossible for there ever to be agreement on the meaning of the term. It is sometimes asserted that privacy is an 'essentially contested concept', meaning that it is so complex and value-laden that disputes regarding its definition cannot be resolved rationally.[24] However, as Andrew Mason has convincingly argued, acknowledging that more than one interpretation of a contested concept may be reasonably held does not necessarily rule out adopting a particular version of the concept as superior to others.[25]

There is no doubt that, like other concepts such as liberty and democracy, the value placed on privacy is culturally and historically relative.[26] However, the problem with privacy is that it has been difficult even to attribute generally accepted culturally and historically specific meanings to the concept. This can only be explained by investigating the relationship between privacy and social developments since the 17th century, looking in particular at the emergence of the modern state and market economy, and the development of modern individualism. In other words, we need to understand the relationship between the Enlightenment political tradition, from Thomas Hobbes to Immanuel Kant, in which privacy played no explicit role, and contemporary political debates, in which privacy is centrally important.[27]

22 Carolyn Doyle and Mirko Bagaric, for example, state that '[t]o define a term or concept is to set out the necessary and sufficient conditions which demarcate the correct usage of the term or concept': Carolyn Doyle and Mirko Bagaric, 'The Right to Privacy and Corporations' (2003) 31 *Australian Business Law Review* 237, 238.

23 Daniel Solove, for example, has suggested that the debate about the meaning of privacy has failed because theoreticians have persisted in attempting to isolate some 'core' meaning, rather than following Wittgenstein in examining 'family resemblances' between related concepts in particular contexts: Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1096–9.

24 Colin Bennett and Rebecca Grant, for example, have argued that 'it would be misleading and confining even to try to provide a general definition of "privacy" to focus the analysis. … More than thirty years of semantic and philosophical analysis leaves us with the overwhelming sense that privacy is a deeply and essentially contested concept': Colin Bennett and Rebecca Grant, 'Introduction' in Colin Bennett and Rebecca Grant (eds), *Visions of Privacy: Policy Choices for the Digital Age* (1999) 3, 5. The notion of an 'essentially contested concept' was introduced by the political theorist W B Gallie: W B Gallie, 'Essentially Contested Concepts' (1955–56) 56 *Proceedings of the Aristotelian Society* 167; W B Gallie, *Philosophy and the Historical Understanding* (1964).

25 As Mason explains, '[a] belief that some conception is better than its rivals may be warranted by the reasons in favour of it even though others reasonably deny that it is the best available': Andrew Mason, *Explaining Political Disagreement* (1993) 55.

26 DeCew has argued that 'it may well be that one of the difficulties in defining the realm of the private is that privacy is a notion that is strongly culturally relative, contingent on such factors as economics as well as technology available in a given cultural domain': Judith DeCew, *Privacy* (2002) The Stanford Encyclopedia of Philosophy <http://plato.stanford.edu/entries/privacy>.

27 H J McCloskey has pointed out that '[t]he absence of serious discussion of privacy is one of the most remarkable features of the writings of such British liberals as J S Mill, Spencer, Hobhouse, and Tawney': H J McCloskey, 'The Political Ideal of Privacy' (1971) 21 *Philosophical Quarterly* 303, 304–5.

The Enlightenment political tradition was essentially concerned with defining the limits of legitimate, as opposed to arbitrary, authority. The main problem posed by the Enlightenment tradition was the problem of sovereignty: given that political authority was not absolute, how could its exercise be justified? The general response was that an exercise of power was legitimate if it was in accordance with law. The establishment of the limits of lawful authority therefore went hand-in-hand with the definition of legal rights of individuals as against the state. In other words, the relationship between the individual and the state was characteristically expressed in legal or juridical terms.

An important area in which the legal limits of state power were defined in the 18th century concerned the state's powers to enter premises and seize property. In the famous 1765 English decision of *Entick v Carrington*,[28] which is commonly regarded as an early decision on 'privacy', Lord Camden CJ ruled against the use of 'general warrants' to search premises and seize papers.[29] Similarly, as Daniel Solove points out, at the time of the Revolutionary War in the United States, 'the central privacy issue was freedom from government intrusion. The Founders detested the use of general warrants and writs of assistance.'[30]

At the time, legal restraints on the intrusion of public authorities into private homes were conceived as part of a general struggle for individual liberties against repressive state power, and not in terms of protecting privacy. However, focusing only on this historically specific struggle for liberty gives a seriously incomplete picture. Although the attention of Enlightenment theorists was directed at defining the legal limits of public authority, as Michel Foucault has pointed out, the growth of the modern state was accompanied by innovative techniques of social control concentrated on ordering individuals and their behaviour.[31]

B *A Foucauldian Analysis of the Definitional Issue*

In his work of the 1970s, Foucault suggested that the Enlightenment focus on legitimate authority and the rights of individuals was based on an inadequate understanding of power and of the way in which power is exercised. In his view, conceiving power solely in terms of a struggle between state repression and individual liberties ignores more insidious techniques through which power is exercised in everyday life. As Foucault explained:

> In defining the effects of power as repression, one adopts a purely juridical conception of such power, one identifies power with a law that says no — power is taken, above all, as carrying the force of a prohibition. Now, I believe that this is a wholly negative, narrow, skeletal conception of power, one that has been curiously widespread. If power were never anything but repressive, if it

[28] (1765) 2 Wils KB 275; 95 ER 807.

[29] For the development of English law relating to powers of entry, see David Feldman, *The Law Relating to Entry, Search and Seizure* (1986) 1–15.

[30] Solove, 'The Origins and Growth of Information Privacy Law', above n 17, 34.

[31] See especially Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan trans, first published 1975, 1979 ed) [trans of: *Surveiller et Punir: Naissance de la Prison*]; Michel Foucault, *The History of Sexuality* (Robert Hurley trans, first published 1976, 1979 ed) [trans of: *Histoire de la Sexualité*].

> never did anything but to say no, do you really think one would be brought to obey it? What makes power hold good, what makes it accepted, is simply the fact that it doesn't only weigh on us as a force that says no; it also traverses and produces things, it induces pleasure, forms knowledge, produces discourse.[32]

Foucault's analysis of power may assist in explaining some of the difficulties encountered with the concept of privacy. First, the concept was not explicitly addressed by Enlightenment political thinkers because their attention was elsewhere. Foucault, in fact, suggested that the focus on the formulation of legal rights and liberties can be seen as essential to the acceptable operation of techniques of social control at the micropolitical level, claiming that 'power is tolerable only on condition that it mask a substantial part of itself.'[33]

Secondly, the concept of privacy is difficult to pin down because it is concerned with techniques of power that are dispersed within society, and which take a diversity of forms. In a process Foucault referred to as 'swarming', techniques of social control were first developed in institutions such as prisons, schools and factories, then became generalised in a variety of contexts.[34] Given the diversity of social practices that give rise to privacy concerns, it is not surprising that different theorists have emphasised different aspects of privacy, highlighting particular concerns in particular contexts. If power relations are everywhere, then privacy, which must be seen in the context of such relations, is an understandably diffuse concept, capable of multiple meanings.

Thirdly, privacy is a complex concept because it is concerned not only with impersonal processes of social ordering, but with the creation of particular kinds of individual subjects. Foucault explained the relationship as follows:

> The individual is no doubt the fictitious atom of an 'ideological' representation of society; but he is also a reality fabricated by this specific technology of power that I have called 'discipline' … In fact, power produces; it produces reality; it produces domains of objects and rituals of truth. The individual and the knowledge that may be gained of him belong to this production.[35]

It is standard practice for privacy to be related to the formation of personal identity. As Paul Freund, for example, put it:

> For the individual in his personal relations privacy offers a shelter for the loosening of inhibitions, for self-discovery and self-awareness, self-direction, innovation, groping, nourishment for a feeling of uniqueness and a release from the oppression of commonness.[36]

Nevertheless, the extent to which the concept of privacy is related to power-based struggles over identity, or over particular forms of subjectivity, has

[32] Michel Foucault, 'Truth and Power' in James Faubion (ed), *Power: Essential Works of Foucault* (2002) 111, 120.
[33] Foucault, *The History of Sexuality*, above n 31, 86.
[34] See, eg, Foucault, *Discipline and Punish*, above n 31, 211.
[35] Ibid 194.
[36] Paul Freund, 'Privacy: One Concept or Many' in J Roland Pennock and John Chapman (eds), *Privacy* (1971) 182, 195.

yet to be fully explored. For the moment, it can be observed that insofar as modern forms of identity are complex and multifaceted, then so too is the concept of privacy.

C *The Legal Recognition of Privacy*

Why is it that even though the concept of privacy was ignored during the political discourse accompanying the formation of the modern state, it was later taken up by theorists who spoke of a 'right to privacy', and subsequently expressly recognised in some Western legal systems? In other words, why has the concept of privacy, at particular points in history, been incorporated into legal systems? The answer to this question is necessarily complex.

The concept of privacy began to receive explicit recognition in the Anglo-American world in the second half of the 19th century. Legal concern with privacy in the United States commenced with an 1890 article by Samuel Warren and Louis Brandeis, which was concerned with public disclosure of private matters.[37] One way to view these concerns, of which the Warren and Brandeis article is a prominent example, is as a response to the progressive intensification and democratisation of techniques of social ordering, including practices of normalisation and surveillance. Intensification and democratisation became possible, in part, either because of new technologies, including communications technologies, or because of new ways of using established technologies.

Warren and Brandeis were specifically concerned with practices made possible by hand-held cameras and by sensational journalism. These practices can be seen as forms of objectification of individual identity. Reporting the activities of private individuals by the press, for example, can be seen as part of the reinforcement and formation of social norms. Concern with these practices prompted Warren and Brandeis to call for legal limits on the surveillance and normalisation that were practised not by the state, but by private parties, especially the press. The authors famously distinguished the relationship between their argument and traditional limits on search and seizure by asking: 'Shall the courts … close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?'[38]

Laws protecting privacy, then, can be seen as a response to crises in the deployment of technologies and associated techniques of social control. In other words, there are times when the proliferation of such techniques becomes so intense that they result in social and political responses. The conventional response, modelled on traditional political analysis of the response to the growth of the modern state, has been to establish legal limits on technologies of social control such as surveillance, documentation and normalisation. As restraints were sought to be placed on diffuse and diverse social practices — not on centralised, repressive state power — they were not sought in the name of 'liberty', but of 'privacy'.

[37] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
[38] Ibid 220.

Nevertheless, the arguments for the protection of privacy were quite naturally assimilated into conventional rationales for political rights, meaning debates concerning the concept of privacy were grafted onto existing political discourse concerning the relationship between individual and state. The process is similar, in fact, to that identified by William Galston, who suggests an analogy between the treatment of sexual relations under the United States constitutional 'right to privacy' and the traditional legal immunity conferred on matters of religious conscience.[39]

Foucault rejected the Enlightenment concept that individuals could be liberated by an appeal to formal, legal rights. His criticism was that this is an inadequate way of framing political questions for two related reasons. First, an appeal to rights is also an appeal to a particular form of universalist, transcendental reason which purportedly grounds legitimate limits on power.[40] Secondly, he argued that an appeal to abstract rights obscures the actual operation of power, while reinforcing the anachronistic concept of power as something held by the sovereign.[41] In other words, Foucault saw the formal juristic mode of analysis and micro-technologies of social ordering as inextricably linked, but with the disciplinary and regulative force of the micro-technologies overwhelming legal limits on sovereign power.[42]

Foucault's objections to an analysis based on universal rights do not, however, exclude the view that legal rights are an integral part of strategies of domination and resistance. As Colin Gordon has explained:

> The deployment and application of law is, for Foucault, like everything else, not good or evil in itself, capable of acting in the framework of liberalism as an instrument for economizing and moderating the interventions of governmental power, necessary as an indispensable restraint on power in some contexts, uses, and guises; it is to be resisted as an encroaching menace in others.[43]

It is therefore possible to see the legal recognition of privacy as part of broader historical struggles for individual identity within totalising forms of political rationality. At times, the struggle is reflected in the recognition of legal limits on particular practices of social control. The timing of the establishment of legal limits may be related to responses to technologies and techniques that challenge conventional understandings of individual subjectivity. Thus, in late 19th century America, intensified press scrutiny challenged conventional notions of those aspects of an individual's life that were 'private', and those that were 'public'. Similarly, the techniques of social control used by mid-20th century totalitarianism were a major challenge to the self-understanding of subjects as free indi-

39 William Galston, 'Practical Philosophy and the Bill of Rights: Perspectives on Some Contemporary Issues' in Michael Lacey and Knud Haakonssen (eds), *A Culture of Rights* (1991) 215, 221.

40 See, eg, Foucault, 'Truth and Power', above n 32; Michel Foucault, 'The Subject and Power' in James Faubion (ed), *Power: Essential Works of Foucault* (2002) 326; Joseph Rouse, 'Power/Knowledge' in Gary Gutting (ed), *The Cambridge Companion to Foucault* (1994) 92.

41 See, eg, Foucault, 'Truth and Power', above n 32; Michel Foucault, 'The Subject and Power', above n 40.

42 See, eg, Foucault, *Discipline and Punish*, above n 31, 223.

43 Colin Gordon, 'Introduction' in James Faubion (ed), *Power: Essential Works of Foucault* (2002) xi, xxxi.

viduals. One response to this challenge was the emergence of international and European human rights instruments, which expressly incorporated rights to privacy.[44]

A comparable development can be seen in the emergence of information privacy laws in response to the widespread use of computers in the automated processing of personal information for the purposes of administration. It is possible to see similar crises emerging in the related deployment of new technologies — such as identity-related technologies (including radio frequency-based identity devices ('RFID') and biometrics), location-based services and 'ambient intelligence technologies' — as well as in the political response to terrorism.[45] It may be that the current challenges will also result in future forms of legal intervention. At the same time, the inherent vulnerability of legal forms of protection of privacy, in the face of processes of social ordering in the name of public welfare and security, needs to be acknowledged. In the current climate, the protection of privacy remains a continual process of negotiating limits, including legal limits, on a broad front: that of individual identities.

D *Understanding the Legal Protection of Privacy*

What does this analysis mean for the way in which we understand the legal protection of privacy?

First, legal protections given to privacy should not be regarded as protecting a transcendental, universal human essence. Rather, privacy laws can be usefully analysed as part of ongoing, historically-specific struggles over identity and forms of subjectivity, in the midst of totalising forms of social ordering. Sometimes privacy laws may entrench particular forms of subjectivity; sometimes they can be seen as part of complex struggles over diverse forms of subjectivity.

Secondly, following from this, privacy laws are an essential part of a social process of continual questioning of what it is to be human subjects. In other words, privacy is related both to a particular form of individuality that is integrated within overall patterns of social control and to forms of subjectivity that resist integration. As Foucault famously expressed this concept:

> Maybe the target nowadays is not to discover what we are, but to refuse what we are. … We have to promote new forms of subjectivity through the refusal of this kind of individuality which has been imposed on us for several centuries.[46]

For these reasons — because privacy is a focal point for political struggles over identity and because the struggles take place, in part, through privacy laws — the legal protection of privacy is a litmus test for the orientation of contemporary legal systems. In this sense, privacy can be seen as a regulatory principle

[44] See, eg, Mark Janis, Richard Kay and Anthony Bradley, *European Human Rights Law: Text and Materials* (1995) 229.

[45] See, eg, Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Doc No EUR 20823 EN (2003).

[46] Michel Foucault, 'The Subject and Power' in Hubert Dreyfus and Paul Rabinow, *Michel Foucault: Beyond Structuralism and Hermeneutics* (1983) 208, 216.

between notions of the self as both determining and determined, as both autonomous and irredeemably dependent on the collective. To the extent that they are inherently associated with the paradoxical nature of modern individuality, privacy laws are also paradoxical: they simultaneously protect the ability of individuals to be self-defining, while also entrenching a particular, universalising notion of the self as a self-defining individual.

Privacy therefore belongs at the very centre of social and political struggles in contemporary, pluralistic societies. Moreover, the centrality of struggles over privacy allows us to understand the persistent tendency for privacy to colonise other rights, or to expand into a more general right of individual autonomy. This is seen clearly, for example, in the famous dissenting judgment of Brandeis J in *Olmstead v United States*, where his Honour referred to privacy as the 'right to be let alone — the most comprehensive of rights and the right most valued by civilized men.'[47] A similar tendency is observed in decisions interpreting the privacy provisions in human rights treaties and conventions. In interpreting art 17 of the *International Covenant on Civil and Political Rights*, for example, the United Nations Human Rights Committee has stated that privacy includes a 'sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone.'[48]

This tendency for privacy to be construed as a general right to autonomy, thereby threatening to swallow other human rights, is explicable by the extent to which complex struggles over individual identity have, since the late 19th century, come to replace struggles for political liberty against repressive state power. Far from being an obscure or peripheral concept, the elusive nature of privacy results from the extent to which privacy is inextricably bound to complex debates over political and administrative rationality, human reason, individuality and forms of subjectivity — debates that have become central to modern Western political and philosophical traditions since, at least, the work of Friedrich Nietzsche. Given that power in modern Western societies is polyvalent and dispersed, not centralised and monolithic, the concept of privacy is likewise polymorphous and diffuse. The legal protection of individual privacy therefore promises not liberation from oppression, but merely ongoing struggles over identity.

III PRIVACY AND ITS VALUES

It is important to distinguish the problems with defining the concept of privacy from the justifications for the protection of privacy.

Identifying the values underpinning the protection of privacy necessarily presupposes contested views concerning human nature and the nature of society. The process of analysis cannot be aimed at uncovering universal values underlying privacy any more than it can be aimed at deriving a universal definition of

47 277 US 438, 478 (1927).

48 *Coeriel and Aurik v The Netherlands*, United Nations Human Rights Committee, 52nd sess, [10.2], UN Doc CCPR/C/52/D/453/1991 (1991).

the concept of privacy. All that we can hope for is to draw on existing analyses of the concept of privacy and its social role in order to see where that leads.

To begin with, it is necessary to explain the basic distinctions drawn in the privacy literature. The first essential distinction that has been made by privacy theorists is between reductionist and coherentist accounts of privacy.[49] Reductionists argue that privacy is neither a single coherent concept nor a distinctive concept. According to reductionist views, therefore, privacy is reducible to other, more fundamental, concepts. Coherentists, on the other hand, maintain that the concept of privacy is intelligible because it is both coherent and distinctive.

Within coherentist accounts of privacy, a further basic distinction must be made between deontological and consequentialist accounts. Consequentialist approaches, commonly associated with some form of utilitarianism, assess the value of actions by first determining what is 'good', then defining 'the right' as that which promotes 'the good'.[50] Deontological approaches, on the other hand, consider 'right' outcomes to be independent of whether or not the actions promote 'good' outcomes.

Although the distinction between deontological and consequentialist approaches is of fundamental importance in evaluating claims for the legal protection of privacy, it has often been poorly made by privacy theorists. It is therefore worth reiterating the basic features of each approach. For theorists who adopt a deontological position, the value of privacy is determined by the extent to which it is consistent with fundamental moral duties, not by the extent to which legal protection of privacy promotes desirable results, such as maximising social welfare. More specifically, the contrast between the two approaches can be seen as a choice between policies which have the objectives of maximising social welfare (usually conceived as the aggregate of summed utilities), and policies based on the protection of fundamental rights. As the unconstrained pursuit of welfare may infringe rights, there is an inherent tension between rights-based and utility-based approaches. In other words, rights-based approaches appear, at the very least, to entail the imposition of constraints on purely welfare-maximising policies.

In this part of the article, reductionist, deontological and consequentialist accounts of the value of privacy are explained and assessed. The implications of deontological and consequentialist accounts of privacy are then considered, and some conclusions drawn.

A *Reductionism*

The most influential reductionist account of privacy was advanced by the American philosopher Judith Jarvis Thomson.[51] Thomson examined a number of factual situations that would conventionally be regarded as invasions of privacy, such as examining someone's personal picture or eavesdropping on a conversation. In each case, Thomson concluded that there was an invasion of some other

[49] See Schoeman, above n 15, 5–6.
[50] See, eg, John Rawls, *A Theory of Justice* (1971) 24–30.
[51] Judith Jarvis Thomson, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295.

protected interest, such as property rights, rights to the integrity and physical safety of the person, or established rights of confidentiality.[52] For the purposes of simplification, Thomson recommended abandoning the search for a coherent concept of privacy in favour of focusing on less contentious rights, especially property rights and rights over the person.

Thomson's argument rests on two propositions: first, that the various claims to privacy rights have nothing in common, such that the concept is incoherent; and secondly, that claims to privacy rights are not distinctive, but are reducible to claims to more fundamental rights, principally property rights and rights over the person.[53] Taking the second proposition first, Thomson's argument is clearly based on an over-expansive view of what is encompassed by property rights and rights over the person. For example, Thomson suggests that property rights include the right that one's possessions not be looked at, and that rights over the person include rights not to be looked at or to be overheard. In other words, claims to property rights or rights over one's person may be exhausted without exhausting all claims to privacy rights. Moreover, claims to privacy rights may be less extensive than claims to property rights or rights over the person.[54] For instance, picking up and taking a pen may infringe a property right, but hardly seems to implicate any claims the owner might have to privacy.

Even if it were conceded that privacy rights are derivative, it does not necessarily follow that claims to privacy rights are incoherent. Determining whether there is something coherent about claims to privacy, however, ultimately depends upon the view adopted as to the social value of privacy.[55] In any case, it is sufficient to note that reductionist accounts, including the arguments advanced by Thomson, completely fail to capture the sense in which the concept of privacy is conventionally used in everyday language, quite apart from the technical, philosophical and legal literature. In other words, reductionists like Thomson are asking us to strain our understanding of the term 'privacy' beyond the limits of credibility.

If we accept the argument advanced above — that privacy is related to rationalising and normalising social practices — then the concept can hardly be confined to property rights and rights over the person, unless the concepts of property and the person are stretched beyond accepted meanings. By suggesting that privacy rights are reducible to property rights or rights over the person, Thomson ignores the most distinctive features of the social, political and legal discourses concerning privacy.

52 Ibid 306–10.

53 Ibid 312–14.

54 Julie Inness, *Privacy, Intimacy, and Isolation* (1992) 33–5.

55 As Jeffrey Reiman puts it,

> even if privacy rights were a grab-bag of property and personal rights, it might still be revealing, as well as helpful, in the resolution of difficult moral conflicts to determine whether there is anything unique that this grab-bag protects that makes it worthy of distinction from the full field of property and personal rights.

Jeffrey Reiman, 'Privacy, Intimacy, and Personhood' in Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 300, 301.

B *Deontological Justifications*

Deontological approaches to privacy emphasise the value placed on the autonomy and dignity of human beings and are, therefore, closely aligned with rights-based approaches.[56]

Those who adopt a deontological approach to the value of privacy invariably hold particular conceptions of what it is to be a 'moral person', in the sense in which that term is used in positions derived from Kantian ethics; that is, a person with desirable moral qualities, such as autonomy, rationality and the ability to enter meaningful relations with others. The best examples of deontological approaches to privacy may be found in the work of Charles Fried, Stanley Benn and Jeffrey Reiman, which will be discussed below.

Fried maintained that the concept of privacy is ultimately referable to a 'principle of morality', which consists of 'the equal liberty of each person to define and pursue his values free from undesired impingements by others'.[57] An important corollary of this principle is that each person should be entitled to the respect of others to pursue his or her values unhindered, which Fried contended is an essential part of being a person. Fried argued that respect for others is necessarily associated with relationships of love, friendship and trust. The ability to enter into these relationships, in turn, depends upon the ability of a person to control private information and, so, to selectively reveal that information to intimate others.

According to Fried, then, privacy is valued because it is a necessary precondition for the formation of intimate relations, and essential to our concept of what it means to be a person.[58] Fried was explicit about the Kantian origins of his account:

> The view of morality upon which my conception of privacy rests is one which recognizes basic rights in persons, rights to which all are entitled equally, by virtue of their status as persons. … In this sense, the view is Kantian; it requires recognition of persons as ends, and forbids the overriding of their most fundamental interests for the purpose of maximizing the happiness or welfare of all.[59]

[56] As Neil MacCormick maintains, 'a theory which asserts the primacy of rights must necessarily postulate that there are goods or values which in their character as goods-which-ought-to-be-secured-to-individuals therefore count as "rights"': Neil MacCormick, *Legal Right and Social Democracy* (1982) 144.

[57] Charles Fried, 'Privacy' (1968) 77 *Yale Law Journal* 475, 479. See also Charles Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (1970). For a similar approach see James Rachels, 'Why Privacy Is Important' in Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (1984) 290.

[58] Fried explains the relationship between privacy and his concept of personhood in the following terms:

> It is my thesis that privacy is not just one possible means among others to insure some other value, but that it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable.

Fried, 'Privacy', above n 57, 477.

[59] Ibid 478.

Benn proposed a deontological account of the value of privacy, while acknowledging the possibility that privacy might also have desirable consequences.[60] The deontological framework for Benn's analysis was set by his central focus on establishing a justification for immunity from uninvited observation, even where there is no discernable harm to the subject. Thus, Benn contended that covert observation of a person is inconsistent with the respect due to each person as a moral being, mainly because covert observation changes the conditions of an activity without the permission of the subject. In outlining his understanding of the relationship between privacy and the fundamental ethical principle of respect for persons, Benn maintained that

> a general principle of privacy might be grounded on the … general principle of respect for persons. By a *person* I understand a subject with a consciousness of himself as agent, one who is capable of having projects, and assessing his achievements in relation to them. To *conceive* someone as a person is to see him as actually or potentially a chooser, as one attempting to steer his own course through the world …[61]

Reiman has also linked privacy to concepts of personhood.[62] In doing so, he was critical of both Fried and Benn. Against Fried, Reiman argued that the ability to selectively withhold information forms too narrow a basis for intimate personal relations, which Reiman suggested are properly based on broader notions of interpersonal caring.[63] Reiman also maintained that individuals have a fundamental interest in privacy separate from the extent to which they are involved with intimate relationships, otherwise those incapable of forming such relationships could not claim a right to privacy.

Reiman considered Benn's view — that privacy is justified by the moral principle of respect for persons as autonomous agents — to be more satisfactory. Nevertheless, Reiman was not persuaded by Benn's argument that, although covert observation is inconsistent with the moral duty of respect for persons, casual observation — for example in a public place — is not inconsistent. Benn had argued that it is not every undesired observation that amounts to a breach of privacy, but only undesired observations of aspects of an individual that are relevant to the person's identity. According to Benn, the content of privacy, being closely related to personal identity, is culture-dependent.[64] Reiman argued,

60 Stanley Benn, 'Privacy, Freedom, and Respect for Persons' in J Roland Pennock and John Chapman (eds), *Privacy* (1971) 1.

61 Ibid 8–9 (emphasis in original). See also at 10, where Benn is explicit in rejecting a consequentialist justification for privacy, asserting that:

> The underpinning of a claim not to be watched without leave will be more general if it can be grounded … on the principle of respect for persons [rather] than on a utilitarian duty to avoid inflicting suffering. That duty may, of course, reinforce the claim in particular instances. But respect for persons will sustain an objection even to secret watching, which may do no actual harm at all.

62 See Reiman, above n 55.

63 Thus, Reiman claims that '[t]he revealing of personal information … is not what constitutes or powers the intimacy. Rather it deepens and fills out, invites and nurtures, the caring that powers the intimacy': ibid 306.

64 As Benn puts it:

> The notion we have of our own extension, of the outer limits of our personalities — those events or situations in respect of which we feel pride or shame — is unquestionably

however, that Benn merely assumed that one is entitled to have aspects of oneself that are related to personal identity exempt from unwanted observation, but failed to show how this follows from the moral principle of respect for persons as autonomous agents.

Thus, while Reiman agreed that the value of privacy is related to the principle of respect for morally autonomous individuals, he disagreed about the reason for this. For Reiman, privacy is essential to the social construction of personal identity because it enables an individual to experience moral ownership of his or her existence.[65] By this, Reiman meant that the ability to control whether or not one's existence becomes part of another's experience allows individuals to form a sense of themselves as separate moral persons. A sense of moral ownership of the self is related to the principle of respect for persons as autonomous agents because it is a precondition of moral autonomy.

Regardless of the differences in emphasis in the above accounts of the value of privacy, all deontological justifications share common features. First, in all of these accounts, privacy is related to the Kantian ethical principle of respect due to others as morally autonomous beings. Privacy, however, is not regarded as identical to moral autonomy, but as important for protecting or promoting autonomy. Secondly, privacy is connected to what it means to be a moral person, meaning a person possessing attributes such as autonomy and rationality. But the precise relationship between privacy and moral personhood varies in the different accounts. According to Fried, the ability to form intimate relations is a necessary attribute of personhood, and privacy is a precondition for intimate relationships. For Benn, respect for privacy is essential to moral personhood insofar as intrusions without consent alter the conditions in which a person can be rationally self-determining (which, on this view, requires information about whether or not one is being observed). Reiman, on the other hand, regards privacy as necessary in order for a person to develop a sense of moral ownership of his or her own experiences, which he regards as a precondition for moral autonomy. Thirdly, privacy is generally not seen as an ultimate value, but has value insofar as it is consistent with, or a condition for, a fundamental deontological rule, such as respect for persons.

Deontological accounts of the value of privacy present an extremely strong case for the protection of privacy in that, on this approach, an invasion of privacy is generally impermissible, even if it would produce 'good' consequences. These views dominated the American privacy literature that emerged from the late 1960s. The argument is essentially that privacy is necessary for individuals to be self-determining and that respect for the privacy of others is essential for human dignity. In this sense, the right to privacy is derivative of the right to respect for persons as morally autonomous beings.

culture-variant; consequently, the application even of a quite general principle of privacy will be affected by culturally variant norms — those regarding family, say, or property.

Benn, above n 60, 13.

65 Thus, Reiman states that '[p]rivacy is a social ritual by means of which an individual's moral title to his existence is conferred': Reiman, above n 55, 310 (emphasis omitted).

Deontological approaches are, however, plagued by a well-known methodological weakness — they are based on culturally and historically contingent notions of personhood, including specific views of the individual subject, autonomy and reason. In particular, there are difficulties in reconciling the view that individuals are radically self-determining with an understanding that individuals are socially constructed. This is related to an underlying tension between the view that privacy is a precondition for moral autonomy, on the one hand, and the view that privacy is necessarily entailed in the principle of respect for human dignity, on the other. The tension arises because violating the principle of respect for others assumes that personal identity is influenced by social norms, whereas moral autonomy assumes independence from social influences.[66] One consequence of this would seem to be that insofar as a person is a morally autonomous individual, the need for the person to be treated with respect diminishes.[67]

As explained in Part II of this article, these difficulties can be addressed by abandoning the formalistic, universalising analysis of privacy favoured by neo-Kantian theorists in favour of a more specific understanding of how claims for the protection of privacy have arisen in the context of struggles over individual identity and power relations exercised through rationalising and normalising practices. Within these processes, deontological justifications for the legal protection of privacy can be seen both as a form of resistance to rationalisation and normalisation, and as a form of entrenching a particular view of the self as atomistic, individualistic and self-determining. This does not mean, however, that deontological justifications of a right to privacy should be ignored; merely that the universalistic pretensions they draw on are overly ambitious.

C *Consequentialist Justifications*

Consequentialist accounts justify privacy insofar as it produces desirable outcomes. Rigorous versions of consequentialism are forms of utilitarianism, whereby outcomes are determined by an aggregation, or maximisation, of individual utilities.

Utilitarian-influenced approaches are well-suited to evaluating which of a number of competing interests should prevail by reference to overall results. For example, a strict consequentialist could have no objection to an invasion of privacy that was necessary to produce a desirable outcome, such as the preservation of life or an increase in economic welfare. However, pure forms of consequentialism have considerable difficulties in dealing with arguments that rights should be respected regardless of the consequences.[68] As a simple example, a

[66] As Robert Post expresses the tension, '[p]rivacy as dignity safeguards the socialized aspects of the self; privacy as freedom safeguards the spontaneous, independent, and uniquely individual aspects of the self': Robert Post, 'Three Concepts of Privacy' (2001) 89 *Georgetown Law Journal* 2087, 2095.

[67] Benn addresses this by locating the moral value of personhood in the potential for autonomy, arguing that a person is worthy of respect because of this potential: Benn, above n 60, 26.

[68] John Gray explains the difficulty faced by utilitarianism as follows:

> if whatever has utility can be broken down into units or elements which are subject to measurement or at least comparison by a common standard, then it will always be possible that a

consequentialist might consider acceptable the publication of intimate details of an intercepted telephone conversation or, indeed, the placement of surveillance cameras inside a person's home, if the invasion of privacy results in an increase in overall welfare.

Various strategies have attempted to reconcile consequentialism with rights-based approaches. These strategies commonly involve attempts at improving utilitarianism, often through some form of indirect utilitarianism. Indirect utilitarianism, such as R M Hare's 'rule utilitarianism',[69] splits ethical principles into practical rules that apply to actual conduct and critical principles that are used to evaluate the practical rules.[70] According to such views, utility is best promoted by adopting practical principles, which may include respect for rights, which are then evaluated against the principle of utility. In this sense, then, rights may have a utilitarian justification.

The most prominent example of a utilitarian justification of a basic right is John Stuart Mill's Principle of Liberty.[71] Leaving aside the considerable ambiguities in Mill's formulation, the Principle of Liberty postulates a sphere of 'self-regarding' action that is immune from the interference of others, even if such interference would ordinarily be regarded as increasing overall welfare. Mill adopted this position because of the particular views he developed of happiness as the determinant of welfare. Drawing on the perfectionist tradition of moral thought, from Aristotle to von Humboldt, Mill regarded happiness not merely as the sum of pleasures over pain, but as the ability of the individual to be self-determining and self-improving. Mill's Principle of Liberty is concerned with marking out an inviolable sphere of liberty, or sphere of autonomous decision-making; it is not concerned with privacy. Nevertheless, it is comparatively easy to construct a Mill-like indirect utilitarian justification for privacy. On this view, a sphere of privacy would be regarded as a necessary condition for the promotion of self-determining, autonomous individuals. In truth, a Millian justification for the value of privacy is therefore difficult to distinguish from deontological justifications.

However, those who have favoured explicitly consequentialist views of privacy have generally not been indirect utilitarians. H J McCloskey, for example, simply regarded the protection of privacy as justified to the extent that it promotes what are, for him, the more fundamental goods of human happiness, justice and liberty.[72] This led him to conclude, in general terms, that if concerns

> very great loss of welfare for one man or a few men can be justified if it produces a great many small increments of welfare for a vast multitude of men. It seems impossible, then, that utilitarian policy should be able to protect the interests of individuals or minorities, when these obstruct the general welfare or the welfare of large numbers. … Basic rights cannot be reduced to utilitarian devices or strategems [sic] without being emptied of their distinctive moral content as expressions of individuals' claims in justice.

John Gray, *Liberalisms: Essays in Political Philosophy* (1989) 120–1. See also David Lyons, 'Utility and Rights' in Jeremy Waldron (ed), *Theories of Rights* (1984) 110, 110–36; Raymond Frey (ed), *Utility and Rights* (1985).

69 R M Hare, 'Ethical Theory and Utilitarianism' in H D Lewis (ed), *Contemporary British Philosophy* (1976) 113.

70 Ibid 123.

71 John Stuart Mill, 'On Liberty' in John Gray (ed), *On Liberty and Other Essays* (1991) 5, 13–14.

72 McCloskey, above n 27, 313.

about privacy come into conflict with more fundamental concerns regarding liberty of action, invasions of privacy should be accepted, and social attitudes adjusted accordingly.

The discipline of modern welfare economics, based on the standard of Pareto optimality, is a much more rigorous form of analysis than other consequentialist accounts of privacy. Responding to the difficulties of comparing interpersonal utilities, Pareto developed a criterion that is indifferent to interpersonal comparisons.[73] Under this standard, if a change in resource allocation would increase the welfare of at least one individual, and not decrease the welfare of any other individual, the change is desirable and is known as Pareto superior. If it is impossible to make any such improvements in resource allocation the situation is known as Pareto optimal.[74] Some of the weaknesses of this approach are, however, evident from Richard Posner's treatment of privacy.[75]

Posner restricted his focus to the economics of personal information, which he held has value only insofar as it results in an increase in welfare. He argued that an individual should be able to prevent the unauthorised disclosure of personal information if this would undermine incentives for the production of that information.[76] Unlike commercial information, such as trade secrets, personal information is generally not costly to produce. As such, making it freely available is unlikely to undermine incentives. On the other hand, Posner contended that non-disclosure of personal information often entails social costs. Such costs include the costs that may be imposed by the individual being able to mislead those with whom he or she deals.[77] Moreover, Posner argued that where others (such as a magazine publisher) value personal information more highly than the data subject, if transaction costs are high relative to the value of the information, rights to the information should be assigned away from the data subject.[78] Where the social costs of not protecting personal information outweigh the social benefits of disclosure, however, Posner maintained that the law should prevent unauthorised disclosure.[79]

In this respect, Posner argued that if private communications were not protected by the law, social costs would generally outweigh any benefits of disclosure. These social costs would include the steps taken to prevent eavesdropping, which would impede effective communications, and presumably the uneconomic efforts of potential eavesdroppers to circumvent attempts at protecting private

[73] The difficulties economists encountered with interpersonal comparisons were associated with the positivist view that it is impossible to compare mental states. See, eg, W Stanley Jevons, suggesting that '[e]very mind is thus inscrutable to every other mind, and no common denominator of feeling seems to be possible': W Stanley Jevons, *The Theory of Political Economy* (3rd ed, 1888) 14.

[74] See, eg, Charles Rowley, 'Public Choice and the Economic Analysis of Law' in Nicholas Mercuro (ed), *Law and Economics* (1989) 123, 130.

[75] See Richard Posner, 'The Right of Privacy' (1978) 12 *Georgia Law Review* 393; Richard Posner, 'Privacy, Secrecy, and Reputation' (1979) 28 *Buffalo Law Review* 1.

[76] Posner, 'The Right of Privacy', above n 75, 397–8.

[77] Ibid 399–401.

[78] Ibid 398–9.

[79] Ibid 403–4.

communications. On the other hand, if a communication lacks social value, such as a private discussion between criminals, Posner concluded that surveillance is justified.

Although this form of analysis provides clear criteria for assessing alternative policy formulations, it is beset by well-rehearsed difficulties facing much consequentialist thinking, especially forms of analysis derived from utilitarianism. A fundamental difficulty is that impersonal social goals always outweigh the interests and values of particular individuals.[80] This criticism has a number of dimensions.[81] First, traditional welfarism requires the interest of the individual to be sacrificed where this would be necessary to maximise overall welfare. Secondly, a focus on maximising the sum of utilities means that distributional concerns are excluded from the analysis. Thirdly, welfarism conflates analysis of what may be rationally maximising for an individual with what is rationally maximising for society. In other words, although it may be rational for an individual to suffer a short-term loss of utility in return for a long-term increase in utility, this does not necessarily mean that it is rational for the utility of one person to be sacrificed for a greater increase in the utility of others.[82]

Like deontological justifications, consequentialist accounts are plagued by universalistic, ahistorical views of what it is to be a human subject. In the case of consequentialism, however, these views determine the goal to which behaviour is directed rather than what amounts to a right action. Most welfare economics, for example, is characterised by the proposition that, under certain conditions, social welfare is maximised by individuals pursuing their self-interest, narrowly defined to exclude considerations relating to the interests of others or to procedural fairness. As Amartya Sen has pointed out, these assumptions are arbitrary and are based on an exceedingly narrow view of rational behaviour.[83] Moreover, as Sen further explained, conventional welfare economics conflates the goal of individual behaviour with the desired outcome, both of which are defined as 'utility maximisation'.[84]

This is inadequate in a number of respects. First, it is inaccurate to regard rational behaviour as entirely self-interested, as a rational individual may clearly take other considerations into account in formulating choices, such as the interests of others or fairness of procedures. In other words, a rational individual may well make choices that do not result in the maximisation of his or her utility. Secondly, and perhaps more importantly, this unduly narrow approach undermines the ability of a rational individual to make a reasoned assessment of goals and values.

[80] Rawls famously expressed this objection: 'Utilitarianism does not take seriously the distinction between persons': Rawls, above n 50, 27.

[81] For the classic exposition, see H L A Hart, 'Between Utility and Rights' (1979) 79 *Columbia Law Review* 828.

[82] See ibid 831, where Hart makes this objection:

> In its misleading analogy with an individual's prudence, maximising utilitarianism not merely treats one person's pleasure as replaceable by some greater pleasure of that same person, as prudence requires, but it also treats the pleasure or happiness of one individual as similarly replaceable without limit by the greater pleasure of other individuals.

[83] Amartya Sen, *Rationality and Freedom* (2002) 3–52.

[84] Ibid 27.

Adopting this perspective helps to explain how the low value placed on individual control of personal information in Posner's analysis results from a form of definitional legerdemain which is characteristic of much economically-influenced analysis. First, Posner ignores individual preferences for preventing disclosure of personal information by defining utility purely in terms of monetary value, thereby denying that personal information has value for the individual. Secondly, Posner does not consider individual preferences that place some value on a social order in which individual control of personal information is respected. Thirdly, Posner excludes essentially deontological considerations relating to the value of a society which accords respect to individual decision-making. Fourthly, Posner's analysis fails to account for the extent to which some control of personal information may be relevant to the ability of individuals to make future decisions, or to be rationally self-determining.

If privacy is understood within the context of overall social processes of rationalisation and normalisation, and as integral to struggles over self-definition, the difficulties consequentialist accounts face in taking privacy seriously are comprehensible. In particular, by valuing a purely instrumental concept of reason, welfarism can be seen as privileging impersonal social objectives over human values, such as the ability of individual subjects to define themselves and respect for human dignity. Strict welfarist analysis is therefore completely implicated in processes of rationalisation and normalisation, suggesting that it is especially ill-suited as a means for analysing the value of privacy. It is only if the models of the individual subject and of human reason underlying welfarism are enriched in ways suggested by Mill and Sen — by including values such as the ability of the individual to determine his or her own ends — that consequentialism is ever likely to be sympathetic to privacy. The implication of such a broad approach would be to constrain the untrammelled pursuit of welfarist objectives by the protection of individual rights, however formulated. However, broadening the approach in this way would seem to introduce the universalistic pretensions that plague deontological approaches to privacy.

D *Australia as a Consequentialist Society*

The generally unsympathetic treatment of privacy by the Australian legal system, including the failure to recognise a right to privacy, is linked to the overwhelmingly consequentialist orientation of Anglo-Australian society, as well as the traditional hostility of Australian common law to recognition of natural rights. In an influential 1985 article, Hugh Collins argued that the dominant features of Australian legal and political ideology conformed closely to Jeremy Bentham's political philosophy, especially its commitment to utilitarianism, legalism and positivism.[85] Collins commented that:

> Customary observations on Australia's political habits reflect the distinguishing characteristics of the Benthamite ideology. Thus, from Bryce onwards, observers have remarked on the attachment to interests rather than ideas in Australian

[85] Hugh Collins, 'Political Ideology in Australia: The Distinctiveness of a Benthamite Society' in Stephen Graubard (ed), *Australia: The Daedalus Symposium* (1985) 147.

> politics. … The utilitarian psychology in Australia legitimizes the pursuit of interest, while the dominance of the ideology negates the possibility of a genuine battle of ideas.[86]

If some recent academic commentary on privacy is any indication, little has changed since this statement was written. For example, in a reversal of deontological justifications for protecting privacy, Carolyn Doyle and Mirko Bagaric argue that unconstrained access by others to one's personal information enhances individual autonomy. In support of this surprising conclusion, they claim that:

> If the whole world knows my address, (natural) hair color, ethnicity, political persuasion and income why will that frustrate my desire to become a professional tennis player, travel overseas, have a family, drink lots of beer most Saturday nights and write the occasional paper? In fact, it is just as likely that the opposite is true. The more that people know about me, the more likely it is that my plans will be realised.[87]

These views would seem not only to embody, in a form of extreme consequentialism, an impoverished understanding of what might be entailed in self-definition, but also a disturbingly monolithic approach to defining desirable social objectives. In short, a society that is obsessed with maximising material welfare is unlikely to be sympathetic to the values underpinning the protection of privacy.

IV THE EMERGENCE OF INFORMATION PRIVACY/DATA PROTECTION LAWS

Privacy laws have developed in distinct historical stages. In the earliest stages, some immunity from interference was guaranteed by laws protecting property rights and rights over the person.[88] This was generally sufficient, given the accepted social understandings and levels of technological development at the time. The development of privacy laws has always been related to both changing social and cultural understandings of the value of privacy and to technological developments.[89] This part of the article concentrates on the most recent stage inthe evolution of privacy laws — the emergence of information privacy (or data protection) laws — and considers the relationship of such laws to the general concept of privacy.

[86] Ibid 155.

[87] Doyle and Bagaric, above n 22, 247.

[88] See 'The Right to Privacy in Nineteenth Century America' (1981) 94 *Harvard Law Review* 1892.

[89] Joseph Rosenbaum has commented that '[o]ur notion of privacy has been and always will be a moving target — dependent on technological capability, societal values and cultural norms': Joseph Rosenbaum, 'Privacy on the Internet: Whose Information Is It Anyway?' (1998) 38 *Jurimetrics Journal* 565, 566.

A *The Emergence of Information Privacy/Data Protection Laws in the United States and Europe*

From the 19th century, government and business administration has been increasingly reliant upon information management systems, initially paper-based, and then later involving automated punch card systems.[90] In the late 19th and early 20th centuries, there were considerable advances in the development of techniques for more efficient processing of paper-based information, such as Hollerith's tabulating device for processing punched cards with census information.[91] Paper-based techniques for information management were, however, completely revolutionised by the stored-program computer, which began to come into use from the late 1950s. The use of the computer for information management drew upon previous conceptions of 'information processing' as a form of mass production.[92]

The post-World War II period saw the emergence of the welfare state, and a corresponding increase in the need for efficient information collection and processing for social planning purposes. The computer was seen as a means of improving rational information management techniques, eventually leading to proposals for the introduction of large national databanks of personal information.[93] In the United States, government agencies, responding to the need to deal with large amounts of information, were instrumental in the early commercialisation of the then unproven machine. As Paul Ceruzzi has pointed out, '[t]he first customers for commercial computers were military or government agencies, who hoped these machines could manage the information that was paralyzing their operations'.[94] Thereafter, United States government agencies and private sector organisations that held large amounts of personal information progressively converted their paper files into electronic databases.

A 1965 report of the Social Science Research Council proposed the establishment of a single repository of government statistical information.[95] Although the proposal was rejected, abiding concerns about the misuse of automated data systems led to the appointment of an Advisory Committee on Automated

[90] See, eg, JoAnne Yates, 'Evolving Information Use in Firms, 1850–1920: Ideology and Information Techniques and Technologies' in Lisa Bud-Frierman (ed), *Information Acumen: The Understanding and Use of Knowledge in Modern Business* (1994) 26, 28–36.

[91] See Simson Garfinkel, *Database Nation* (2000) 17–18.

[92] As Philip Agre explains:

> The first methods for representing human activities on computers were derived from the work-rationalization methods that industrial engineers had been developing since the 1910s. Hence the phrase 'information processing': the idea was that computers automate a kind of factory work whose raw material happens to be information rather than anything physical or tangible.

Philip Agre, 'Beyond the Mirror World: Privacy and the Representational Practices of Computing' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997) 29, 33. See also JoAnne Yates, *Control Through Communication: The Rise of System in American Management* (1989).

[93] See Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (1992) 45–53.

[94] Paul Ceruzzi, *A History of Modern Computing* (1998) 10.

[95] 'Privacy and Efficient Government: Proposals for a National Data Center' (1968) 82 *Harvard Law Review* 400, 401.

Personal Data Systems in 1972.[96] The Advisory Committee developed a code of practice, which it termed 'fair information practices', to apply to the collection, storage, use and dissemination of personal information.[97] The Committee's proposals were embodied in the *Privacy Act of 1974*, 5 USC § 552(a) (1988) ('*Privacy Act of 1974*'), which applied the fair information practices to federal government agencies; established penalties for improper disclosure; gave individuals a right of access to their files; and provided an opportunity to correct errors. The code of fair information practices recommended by the Committee and contained in the *Privacy Act of 1974* have been influential in the development of information privacy laws throughout the world.[98]

At the same time that concerns relating to the computerisation of personal information led to the development of fair information practices in the United States, similar concerns resulted in the development of the European concept of 'data protection' (*Datenschutz*).[99] The European legal response was also motivated by proposals to merge separate government databanks into a single repository. For example, in the late 1960s, the Swedish government proposed to merge census, registration and taxation information into a single databank, and in the early 1970s there were similar plans in a number of German states.[100] These proposals led directly to the introduction of the first information privacy laws, notably the data protection law of the German state of Hesse in 1970[101] and the 1973 Swedish *Datalag*.[102]

Unlike the United States' response, the first European laws were not expressly linked to the protection of individual privacy, but were concerned with ensuring that the new techniques of data processing conformed to overall social objectives, including data security and the accuracy of computerised records.[103] The first data protection laws therefore used highly technical terminology, such as 'data bank' and 'data file'. Moreover, as it was envisaged that records would be retained in a relatively small number of large databanks, some of the laws imposed requirements for registration and licensing of databanks.[104]

As Viktor Mayer-Schönberger has explained, as it became clear that data processing would not be confined to a limited number of centralised databanks, the technocentric approach of the initial data protection laws became unsustain-

96 Secretary's Advisory Committee on Automated Personal Data Systems, United States Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens* (1973) ix.

97 See, eg, Robert Gellman, 'Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions' (1993) 6 *Software Law Journal* 199, 210–11; Gellman, 'Does Privacy Law Work?', above n 14, 194–202; James Nehf, 'Recognizing the Societal Value in Information Privacy' (2003) 78 *Washington Law Review* 1.

98 See David Flaherty, *Protecting Privacy in Surveillance Societies* (1989); Bennett, *Regulating Privacy*, above n 93, 70–1, 95–115.

99 See Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997) 219, 219, 221–5.

100 Ibid 222.

101 *Hessisches Datenschutzgesetz*, v 7.10.1970, GVBl Hesse I S 625.

102 *Datalag* (1973:289) (Sweden) (*Data Act*).

103 See Mayer-Schönberger, above n 99, 223.

104 Ibid 224.

able.[105] Instead of regulating such technology, European data protection laws turned towards reinforcing individual rights. Whereas the first data protection laws had provided rights of access and correction, these were seen as necessary mainly to ensure the accuracy of information held in databanks. However, data protection laws passed in the last half of the 1970s, such as the French,[106] Austrian[107] and Norwegian[108] laws, were based on recognising individual rights over personal information, including rights to refuse processing of data for certain purposes (such as direct marketing) and limited rights to prevent dissemination of data. Moreover, a right to information privacy was expressly recognised as a constitutional right in Austria,[109] Spain[110] and Portugal.[111] The second wave of European data protection laws therefore reflected attempts to combine a focus on the process of data management with concerns for protecting individual rights to privacy.

Just as earlier technologies and institutions challenged concepts of individual identity within the context of the integration of individuals into overall social processes of rationalisation and normalisation, the development of computerised processing of personal information in the 1960s and 1970s represented a new, more intense stage in the instrumentalist organisation of society. It seems hardly coincidental that this historical period was characterised by the emergence of the 'politics of identity'. Further, it is not surprising that the computerisation of personal records met with social resistance, including calls for the legal regulation of data processing.

B *How the Different Orientations of the American and European Legal Systems Influenced Approaches to Data Processing*

By the late 1970s, experience with automated processing of personal data resulted in similarities in the European and American approaches to the problem of regulating data protection.[112] There were, however, important differences in the social and political background to the development of information privacy policies in the United States on the one hand, and in Europe on the other.

The European approach to data protection must be seen in the context of the 20th century struggle against totalitarianism. The European experience of mid-20th century totalitarianism resulted in a deep suspicion of any attempts by centralised authorities to increase their capacity for surveillance of individuals. Moreover, the activities of the secret police in the totalitarian regimes of Eastern Europe and the Soviet Union, which focused on monitoring individuals and collecting personal information in extensive (and often inaccurate) filing

105 Ibid 226.
106 *Loi No 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertés* (France).
107 *Datenschutzgesetz* BGBl. 565/1978 (Austria).
108 *Lov om personregistre mm av 9 juni 1978 nr 48* (Norway).
109 *Datenschutzgesetz* BGBl. 565/1978 art 1 (Austria).
110 *Spanish Constitution* art 18.
111 *Portuguese Constitution* art 35.
112 Bennett, *Regulating Privacy*, above n 93, 95–111; Colin Bennett, 'Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997) 99, 99–123.

systems, provided a continuing example of the repressive use of information management techniques.[113] European data protection law is part of the broader European project of building institutions and practices, including the EU itself, which are intended to ensure that the horrors of European totalitarianism are not revisited.[114]

The American approach to information privacy developed from a different social and political tradition. The American polity can be said to be based upon two quite distinct values: the 'liberal' commitment to limited government and the 'republican' emphasis on participation in democratic decision-making.[115] Paul Schwartz, for example, has explained the translation of these values into constitutional norms in the following terms:

> The *United States Constitution* establishes a framework for a debate among citizens about the nation's institutional relationships and fundamental values. One way this document does so is by providing critical controls on the State; its provisions carefully establish the government's structure and limit its behavior. The *Constitution* also contains provisions that indicate concern for individual self-determination. Its Bill of Rights and Civil War Amendments contain the most important language in this regard.[116]

The tension between these two fundamental values is evident in the evolution of information privacy policies in the United States. The first stage of policy development, resulting in the application of fair information practices to personal information held by the public sector pursuant to the *Privacy Act of 1974*, can be seen, in part, as an expression of the liberal suspicion of centralised government and a corresponding preference for imposing limits on state power. At the same time, by introducing individual rights of access and correction, the *Privacy Act of 1974* could be seen as supporting the right of an individual to participate in decisions relating to the management of personal information. The first stage in the development of information privacy law in the United States can therefore be regarded as a response to the threat of automated data processing which drew upon elements of both the liberal and the republican traditions.

C *Transborder Data Flows and the Temporary Convergence of Approaches*

The emergence of national information privacy laws in the late 1970s raised the possibility that inconsistent standards would act as a barrier to the increas-

113 See, eg, Timothy Garton Ash, *The File: A Personal History* (1997). As Paul Schwartz has noted:

> totalitarian regimes in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control. Even without computers, these regimes demonstrated the fragility of the human capacity for self-determination in the face of widespread spying and data collection.

Paul Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 *Iowa Law Review* 553, 560.

114 See, eg, Robert Kagan, *Of Paradise and Power* (2003).

115 See, eg, Bruce Ackerman, *We the People: Foundations* (1991); Joel Reidenberg, 'Setting Standards for Fair Information Practice in the US Private Sector' (1995) 80 *Iowa Law Review* 497, 501; Martin Flaherty, 'History "Lite" in Modern American Constitutionalism' (1995) 95 *Columbia Law Review* 523; Paul Schwartz, 'Internet Privacy and the State' (2000) 32 *Connecticut Law Review* 815.

116 Schwartz, 'Privacy and Participation', above n 113, 566 (citations omitted).

ingly important transfer of data across national borders. This was, nevertheless, also a time marked by considerable policy convergence in the European and American responses to data processing. Colin Bennett has suggested that the factors which led to this policy convergence included the common features of data processing technology and the appearance of an elite group of international policy experts who informally shared approaches and experiences.[117] Bennett explains the process of national policy development in the following terms:

> For the pioneers, the United States and Sweden, the convergence resulted from independent and indigenous analyses that traveled along the same learning curve and arrived at the same conclusion. For West Germany, and other countries such as Canada, France, Norway, Denmark and Austria that legislated in the late 1970s, the convergence followed from the mutual process of lesson drawing within an international policy community. For Britain, and other laggards such as the Netherlands, Japan, and Australia, the convergence has resulted from the pressure to conform to international standards for mainly commercial reasons.[118]

International concerns regarding the adverse consequences of possibly inconsistent national standards led to the drafting of two important international instruments: the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[119] and the Organisation for Economic Co-operation and Development *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ('OECD Guidelines').[120] These instruments reflected a consensus that had emerged in relation to general principles applicable to the collection, storage, use and disclosure of personal information. The general principles, known as 'fair information practices' (the American terminology) or 'data protection principles' (the European terminology), and termed 'First Principles' by Joel Reidenberg,[121] represent an attempt to balance the competing values of information privacy and the free flow of information.

International consensus on the data protection principles represented a considerable achievement, which has resulted in the principles forming the template for all subsequent national information privacy laws. Nevertheless, even at a time of convergence in international policy-making, there were underlying tensions between the fundamental approaches of the United States on the one hand, and Europe on the other. Justice Michael Kirby, who chaired the international Expert Group that was responsible for developing the OECD Guidelines, explained the tensions within the group in the following terms:

> Within the Expert Group there were brilliant antagonists. The chief US delegate, Mr William Fishman, expressed with great clarity the American commitment to the free flow of data and of ideas. The head of the French delegation,

117 Bennett, *Regulating Privacy*, above n 93, 220–50.

118 Ibid 222.

119 Opened for signature 28 January 1981, ETS No 108 (entered into force 1 October 1985).

120 The Preface to the OECD Guidelines refers to 'a danger that disparities in national legislations could hamper the free flow of personal data across frontiers'.

121 See Joel Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review* 1315, 1325.

> Mr Louis Joinet, led those in the Expert Group who were alarmed by the dangers to individual privacy of completely unrestrained collections of personal data, vastly expanded in quantity and kind by the new technology. Each protagonist spoke with sincere conviction and gathered supporters. The contemporary state of technology meant that US business interests stood to gain from the growth of informatics and the spread of transborder data flows. The French and European business interests, on the other hand, coincided generally with restrictions insistent upon privacy protection. Not for the first time, philosophy and law followed trade.[122]

In retrospect, given the different policy motivations behind the American and European approaches, and the fundamentally different orientations of the two social systems, it is not surprising that the consensus resulting in common data protection principles was short lived. The subsequent history of information privacy law is therefore largely one of diverging American and European approaches, which has effectively framed the policy choices facing other jurisdictions considering privacy law reform, including Australia. Before discussing these choices, however, it is necessary to analyse the particular justifications for information privacy laws in greater detail.

V JUSTIFICATIONS FOR INFORMATION PRIVACY/DATA PROTECTION LAWS

As explained in Part II of this article, the introduction of computer and data processing in the 1960s was one of the main reasons for the emergence, at that time, of American legal and philosophical literature dealing with the concept of privacy. This was reflected in the number of privacy theorists who defined privacy relatively narrowly in terms of control of personal information. The practical requirements for the operation of modern governments and markets, however, mean that it is impossible for individuals to assert complete control over their personal information. The objective of information privacy policies must therefore be conceived in terms of balancing individual control over personal information with the instrumental objectives of rational administration and efficient markets.

Assessing justifications for information privacy laws depends upon understanding the extent to which considerations relating to information privacy differ from considerations relating to other forms of privacy. Data processing presents different policy challenges because it is so ubiquitous. To the extent that the functioning of modern societies depends upon the circulation of personal information, purely individualistic forms of legal protection are an inadequate means for dealing with privacy issues arising from data processing.[123] As Bennett has argued:

[122] Justice Michael Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 Years On' (1999) 6 *Privacy Law & Policy Reporter* 25, 25.

[123] Spiros Simitis explains problems arising from the ubiquity and intensity of data processing as follows:

> Modern forms of data collection have altered the privacy discussion in three principal ways. First, privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone. … [Second, information technologies] make it possible

> What is needed is a more holistic perspective that sees data protection as a process that involves a wide network of actors (data users, data subjects, and regulators) all engaged in the co-production of data protection. The successful implementation of data protection requires a shift in organizational culture and citizen behavior. Data protection is a learning exercise that involves a mutual process of education and mediation from the bottom up as much as it involves regulatory command from the top down.[124]

The legal and social mechanisms for dealing with data processing are therefore necessarily different from the mechanisms for dealing with other forms of privacy intrusion.

The legal and social mechanisms for dealing with data processing, which require a degree of comprehensiveness approaching the activity of data processing itself, have built on the 'fair information practices' or 'data protection principles', which establish broad guidelines or standards for the regulation of processes or practices, rather than on hard-edged rules for determining whether an intrusion is actionable. The precise nature of the principles adopted, however, should conform to the particular orientation of the legal and social system in question.

Like general arguments for the legal protection of privacy, the rationales conventionally given for information privacy laws may be divided into deontological and consequentialist justifications. It is important to be clear about how the justifications for information privacy laws differ from justifications for privacy laws more generally.

A *Deontological Justifications for Information Privacy Laws*

As with deontological accounts of the value of privacy more generally, deontological justifications for information privacy laws have been concerned with the potential for data processing to undermine the respect due to individuals as self-determining, autonomous moral agents.

How, then, do deontological objections to data processing differ from deontological accounts of privacy more generally? To begin with, the benefits of data processing are largely the result of the efficiency with which computer technologies enable the collection of relatively small, discrete amounts of personal information and their aggregation into larger, more comprehensive 'dossiers' concerning an individual. Initial responses to the use of the computer in data processing were characterised by Orwellian fears that the compiled information would be misused to increase state control at the expense of the individual. Schwartz expressed these concerns in the following terms:

> to record and reconstruct individual activities in minute detail. Surveillance has thereby lost its exceptional character and has become a more and more routine practice. Finally, personal information is increasingly used to enforce standards of behaviour.

Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 *University of Pennsylvania Law Review* 707, 709–10 (citations omitted).

[124] Bennett, 'Convergence Revisited', above n 112, 119–20.

> In today's information society, extensive collections of data relating to identifiable persons are typically organized in extensive computer data banks. This kind of data processing creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience. Through the use of their data banks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children.[125]

The fears were essentially that the increased information available from data processing could provide the means for the development of totalitarian practices, whereby non-conforming individuals would be somehow marginalised, disciplined or 'disappeared'. The experience of 20th century European totalitarianism provided the context for suspicions of the activities of central governments upon which such fears have arisen. Fears that governments have an in-built propensity to use surveillance technologies against individuals, and particularly against non-conformists, have become almost the standard reaction to any increase in the ability of governments to extend surveillance capabilities. This has been seen recently in the reactions to plans for increased surveillance capabilities following the terrorist attacks of 11 September 2001.[126]

While surveillance capabilities are always open to abuse, the main deontological objections to data processing have not been premised on the possible misuse of information by the state. The concerns have instead been related to data processing as a form of ongoing surveillance or monitoring of individuals, and to how this may foster social conformity. The main objections have centred on the extent to which data processing may result in the collection of detailed information about an individual without the consent (or knowledge) of the individual concerned. This, it is argued, has a propensity to undermine individual autonomy because it alters the conditions upon which individuals make decisions.

The ever-present threat of surveillance through the collection and processing of personal data, which Roger Clarke terms 'dataveillance',[127] thereby inhibits individual decision-making and creates the conditions for a form of self-censorship. David Flaherty, for example, has pointed out that:

> The existence of dossiers containing personal information collected over a long period of time can have a limiting effect on behavior; knowing that participa-

[125] Schwartz, 'Privacy and Participation', above n 113, 560 (citations omitted). These concerns are, if anything, expressed more clearly by Gebhard Rehm's comments:

> In some respects, the situation has become frighteningly similar to George Orwell's *1984* vision of a totalitarian state keeping its citizens under complete surveillance. That an Orwellian society, consisting of degrading human beings to mere objects of state action, is inconsistent with the Kantian idea of man as a rational being, that underlies a democratic society based on the rule of law, hardly needs explanation. But every single move towards a society with more rather than less surveillance also gnaws at Kant's ideal because it leads to more heteronomous decisionmaking.

Gebhard Rehm, 'Just Judicial Activism? Privacy and Informational Self-Determination in US and German Constitutional Law' (2001) 32 *University of West Los Angeles Law Review* 275, 276.

[126] See, eg, Electronic Frontier Foundation, *EFF Review of May 20 Report on Total Information Awareness* (2003) <http://www.eff.org/Privacy/TIA/20030523_tia_report_review.php>.

[127] See Roger Clarke, 'Information Technology and Dataveillance' (1988) 31 *Communications of the ACM* 498.

> tion in an ordinary political activity may lead to surveillance can have a chilling effect on the conduct of a particular individual.[128]

This form of objection to data processing is directly related to Benn's analysis of covert observation, referred to in Part III(B) of this article. For example, in explaining how data processing can inhibit decision-making, Jerry Kang refers to Benn's objections that covert observation 'brings one to a new consciousness of oneself, as something seen through another's eyes.'[129]

Apart from concerns that data processing compromises autonomous decision-making, data processing has been said to undermine human dignity. Since becoming widespread, data processing has been one of the main instruments for increasing bureaucratic rationalisation. The collection and processing of large amounts of personal data has become essential for planning in the public and private sectors. Although necessary to the functioning of modern societies, data processing is a deeply impersonal form of social practice, which entails treating individual data subjects in instrumental terms — as means rather than ends. Moreover, by subsuming the individual data subject into an impersonal bureaucratic process, data processing can be seen as having a normalising effect.[130]

In this sense, then, deontological objections to data processing have some common ground with fears of the potential misuse of increased information in totalitarian practices but are, in fact, quite different. Totalitarian fears are based on the prospect that surveillance will be used by authoritarian regimes to control individual behaviour, especially the behaviour of dissidents. Data processing, however, is not consciously targeted at controlling behaviour or creating social conformity.[131]

Therefore, we can see that deontological objections to data processing, like deontological justifications of privacy more generally, build on essentially Kantian concepts of autonomy and dignity. They differ from general deontological justifications of privacy, however, mainly in the way in which they are directed against impersonal social processes of rationalisation and normalisation, which are seen as undermining individual autonomy, and not at particular invasions of privacy by the state or other individuals. In this sense, as further explored below, deontological objections to data privacy can be linked to the important philosophical and political tradition that is characterised by a fundamental disquiet with the perceived excesses of Western political and administrative rationality and found in thinkers as diverse as Weber, Heidegger, Foucault and Habermas. This is hardly surprising given that, despite the considerable differences between such thinkers, each owes an intellectual debt to Kant.

[128] Flaherty, *Protecting Privacy in Surveillance Societies*, above n 98, 9. Simitis echoes these concerns, claiming that '[i]nhibition … tends to be the rule once automated processing of personal data becomes a normal tool of both government and private enterprises': Simitis, 'Reviewing Privacy in an Information Society', above n 123, 733.

[129] Benn, above n 60, 7, cited in Jerry Kang, 'Information Privacy in Cyberspace Transactions' (1998) *Stanford Law Review* 1193, 1260.

[130] See, eg, Simitis, 'Reviewing Privacy in an Information Society', above n 123, 733.

[131] See, eg, Nehf, above n 97, 12; Daniel Solove, 'Privacy and Power: Computer Databases and Metaphors for Information' (2001) 53 *Stanford Law Review* 1393, 1417.

B *Consequentialist Justifications for Information Privacy Laws*

However the objectives of data protection are specified, data protection laws based on consequentialist considerations must maximise the social benefits of data processing and minimise the costs.[132] This will commonly take the form of a conventional welfarist calculus of costs and benefits, weighing the social benefits of data processing against the interests of individuals about whom the information is collected and processed. In some circumstances, such as where a law is aimed at ensuring the accuracy of information upon which an important decision will be made, the overall social benefit may coincide with the interests of an individual data subject. In other circumstances, however, there may be an apparent conflict between the social benefits of information processing and individual interests. Applying a conventional welfarist analysis to such circumstances will mean that the interest of the individual must be subordinated to overall social welfare.

The social benefits of laws that regulate data processing are easy to explain. Data processing is necessary for the functioning of governments and markets. Government decisions, including decisions relating to individuals and social planning decisions, require access to personal information. Decisions by private firms, including marketing and production decisions, and decisions relating to the provision of credit also require access to personal information. The functions of data processing are compromised to the extent that data are inaccurate, incomplete or of poor quality. Inaccurate, incomplete or poor quality information will result in poor quality business decision-making and poor social planning.

However, the extensive amounts of information that governments and private firms hold about individuals makes it impossible for all of the information to be completely accurate all of the time. Given the costs of information management, tolerance of a certain level of inaccuracy may well be cost-effective for the individual firm or government agency. Decisions made on the basis of poor quality information, however, can have serious consequences for the individual in question, leading, for example, to withdrawal of welfare payments, imposition of fines or failure to obtain credit. Furthermore, if the individual does not have access to the reasons for decisions, it may be difficult to challenge poor decisions made on the basis of poor information. These costs to the individual will also entail flow-on social costs. Information privacy laws therefore have the purely instrumentalist objective of maximising the social benefits of data processing, primarily by ensuring optimal accuracy of the personal information. A common way of expressing this is to say that information privacy laws promote 'good' information management practices.

Consequentialist justifications for information privacy laws depend, of course, on the particular conception of the 'good' adopted. A welfarist approach will be concerned to optimise the efficiency of data processing. Adopting such an approach, a consequentialist justification of information privacy laws differs from consequentialist justifications of privacy in general, in that legal regulation

[132] See, eg, Robert Hahn and Anne Layne-Farrar, 'The Benefits and Costs of Online Privacy Legislation' (2002) 54 *Administrative Law Review* 85, 94–116.

of information privacy may be considered necessary in order to minimise the social costs of data processing. However, if individual preferences for privacy are not factored in, it will be more difficult to formulate a welfarist justification for other forms of privacy law. Following from this, the overwhelmingly consequentialist orientation of the Australian legal system can be seen in the commencement of a comprehensive Commonwealth public sector information privacy law in 1989,[133] and the recent rash of information privacy laws, which can be readily contrasted with the persistent failure to recognise a general right to privacy by either the courts or the legislature.

C *Understanding Approaches to Excessive Rationalisation and Weberian Analysis*

Information privacy or data protection laws based on purely consequentialist considerations have a tendency to become narrowly focused on improving technocratic procedures of information management, rather than addressing the privacy implications of data processing. This tendency is the source of much criticism of current information privacy laws. Simon Davies, for example, has argued that:

> data-protection acts generally have serious limitations. One of the broadest deficiencies is that they are seldom privacy laws. They are information laws, protecting data before people. Instead of being concerned with the full range of privacy and surveillance issues, they deal only with the way personal data is collected, stored, used and accessed.[134]

Yet an information privacy regime must, in the final analysis, choose between maximising the net social benefits of data processing and protecting individual rights. Particular national regimes can be placed on a spectrum between pure rights-based and consequence-based approaches. Rights-based and consequence-based approaches have different implications for the form of information privacy laws, but also represent different responses to the processes of social rationalisation and normalisation which this article has suggested are central to concerns relating to the concept of privacy.

Max Weber was the first to attempt to systematically investigate technocratic rationality, in the sense of the emergence of purely instrumentalist forms of bureaucratic or market processes, along with the tension between technocratic rationality and the Enlightenment ideal of autonomous individuals.[135] Weber's

133 *Privacy Act 1988* (Cth).

134 Simon Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (1997) 143, 156.

135 The discussion in this part focuses on data protection regimes within the context of impersonal bureaucratic processes across both public and private sectors. Given that data protection laws emerged, in part, as a response to transborder data flows of personal information, the effects of the commodification of personal data within the development of global information markets should also be emphasised: see, eg, Michael Hardt and Antonio Negri, *Empire* (2000) 294–300. To give this issue the attention it deserves would require a separate research project. For the purposes of this article, the emphasis is on the continuity of automated procedures for processing personal information and the effects of computerisation on those processes.

concept of rationalisation, which was central to his analysis of Western civilisation, was complex, based on distinctions between purpose-oriented and value-oriented rational action, and formal and substantive rationality.[136] Purpose-oriented rational action is characterised by an approach in which an action is valued as the best means of achieving an end, rather than being valuable in itself. Value-oriented action, on the other hand, is based on a belief in the absolute value of the behaviour itself, irrespective of the consequences. According to Weber, few actual actions are purely oriented in either of these two ways.[137]

Nevertheless, in his analysis of capitalism, Weber saw economic activity as increasingly characterised by purpose-oriented rational action. It was in his analysis of capitalist economic activity that Weber introduced the distinction between formal and substantive rationality. Formal rationality is closely associated with the market, involving the calculation of costs and benefits directed to economic ends.[138] The concept of substantive rationality, on the other hand, is concerned with determining the value of the system as a whole which, for Weber, depended ultimately upon subjective value judgements.[139] Weber was critical of the dominance of purpose-oriented, formal rationality in Western capitalist societies because of what he saw as the overvaluation of economic ends and the erosion of individual freedom.[140] At the same time, Weber was ambiguous about bureaucratic rationalisation, seeing it as indispensable to the efficient administration of modern social systems, but also as profoundly dehumanising, turning the individual into a cog in an impersonal social machine.[141] Weber's response to the irreversible rationalisation of life was essentially that, in a society without objective values, human dignity requires that each individual choose the values by which to live, thereby conferring meaning on life.[142]

From this brief review of Weber's work, it is possible to see how analysis of approaches to data processing can be linked to fundamental tensions within the liberal political tradition. Processes of economic and bureaucratic rationalisation require that continual attention be given to maximising the net benefits of data processing for the overall social good. This, however, assumes that the good is identical to economic efficiency. The liberal attachment to the ideal of individual autonomy, on the other hand, is based on the proposition that individuals should be free to determine their own concept of the good. Insofar as rationalisation is

136 Max Weber, *The Theory of Social and Economic Organization* (A M Henderson and Talcott Parsons trans, 1947 ed) [trans of: *Wirtschaft und Gesellschaft*].

137 Ibid 107.

138 Ibid 184–5.

139 Ibid 185–6.

140 As Gane points out: '[The] shift towards instrumental reason … may, in these terms, be seen as a tragic development, for while it renders social relations more predictable it does so by restricting the basis for creative and meaningful value-rational social action': Nicholas Gane, *Max Weber and Postmodern Theory: Rationalization versus Re-enchantment* (2002) 27.

141 Weber, *The Theory of Social and Economic Organization*, above n 136, 337–41; Max Weber, 'Economy of Law (The Sociology of Law)' in Guenther Roth and Claus Wittich (eds), *Economy and Society: An Outline of Interpretive Sociology* (Fischoff et al trans, 1978 ed) [trans of: *Wirtschaft und Gesellschaft: Grundriss der Verstehenden Soziologie*].

142 See, eg, Max Weber, 'Politics as a Vocation' in H H Gerth and C Wright Mills (eds), *From Max Weber: Essays in Sociology* (1970) 77, 127.

an irreversible feature of modern Western societies, such societies are inevitably caught between these two orientations which, in effect, reflect the fundamental split in the Cartesian subject, between the rational subject and the empirical subject. Information privacy laws are also caught between these two orientations.

D *Consequentialist and Rights-Based Approaches to Excessive Rationalisation in Context*

Information privacy laws that reflect a welfarist, consequentialist approach do not challenge economic and bureaucratic rationalisation; they reinforce it. At the same time, such an approach reflects a particular view of the subject as an atomistic, self-interested individual. Insofar as rationalisation confers social benefits, however, a consequentialist approach is, to an extent, valuable and unavoidable.

The position of information privacy laws that reflect a rights-based, deontological approach is more complex. On this approach, the ability of the data subject to make fundamental decisions about his or her own life demands that he or she have rights over data processing, even if recognition of such rights undermines the efficiency of data processing. At the same time, traditional deontological approaches embody specific, universalistic views of the moral subject and human reason. To the extent that laws embody a particular tradition of moral universalism, they can be seen as privileging certain forms of subjectivity, and thereby also promoting social normalisation.

The problem of how to deal with rationalising and normalising forces within society — forces which, as we have seen, are often characterised as privacy issues — raises central questions concerning the ethical foundations of legal systems within post-Enlightenment societies. In this regard, choices must be made concerning the extent to which it is possible to attempt to rationally reconstruct the Enlightenment project, however imperfectly, or whether any such attempt necessarily entails the dangers of reinforcing totalising forms of power and undermining social pluralism. In other words, can the universalising tendencies of the Western tradition still be seen as somehow liberating, or are they invariably oppressive?

Adopting a Foucauldian perspective, however, the role of the legal system within fragmented, pluralistic societies, whose functioning depends upon extra-legal forms of rationalising power, is fundamentally partial and ambivalent; sometimes limiting rationalisation, sometimes reinforcing it. On the one hand, if a legal system adopts a purely consequentialist, instrumentalist approach to regulatory practices such as data processing, then it can be seen as better integrating individuals within impersonal social processes, while promoting and obscuring the operation of those processes. On the other hand, the adoption of a rights-based approach, especially in a legal system that is fundamentally consequentialist in orientation, is likely to make the values involved in impersonal social processes more transparent. In short, a rights-based approach to regulating data processing may reinforce the integration of individuals within impersonal social processes as much as a consequentialist approach, but may

also promote greater transparency about the social processes themselves, and the possibility of a diversity of social reactions to these processes.

If it is desirable for post-Enlightenment societies to encourage a diversity of views concerning what it means to live in such societies, and a diversity of life choices, then debates concerning the foundations of legal rules regulating rationalising processes must be encouraged. A rights-based approach to regulating data processing should not, therefore, be seen primarily as protecting the freedom of individuals to make their own life choices, but as creating opportunities for debates concerning social processes, especially processes such as data processing that can be characterised as dehumanising or impersonal. The possibilities for such debates are enhanced when individuals have the ability to participate in decisions relating to data processing, or mount legal challenges in relation to specific practices. This improves the understanding of such practices, as well as of the relationship between totalising and rationalising practices and individual identity formation.

VI HISTORICAL DIVERGENCE OF AMERICAN AND EUROPEAN APPROACHES TO INFORMATION PRIVACY/DATA PROTECTION AND THE 'SAFE HARBOR' COMPROMISE

Is it possible to map the main conceptual justifications for information privacy laws, outlined above, to legal approaches taken to information privacy laws? This part of the article commences that task by explaining the increasing differences between the American and European approaches to data processing. Following the brief period of convergence in American and European legal responses to the concerns raised by data processing — which resulted in the adoption of the 'First Principles' as an international standard in the early 1980s — European and American legal approaches to data processing have diverged. The differences in approach are not mere accidents of history, but reflect profoundly different conceptions of the role of government, and of the law, within the European and American social and legal systems.

A *An Outline of the American and European Approaches*

In summary, drawing from the liberal strand of the American political tradition, the United States' approach to information privacy has been predominantly non-interventionist and mainly concerned with protecting individuals from government interference. Flowing from this, United States policy has tended to favour the free flow of information over individual privacy rights. Thus, while the *Privacy Act of 1974* applied the fair information practices to the federal public sector, there is no comprehensive information privacy law applying information privacy principles to the private sector. Instead, information privacy laws have been enacted on an ad hoc basis to deal with problems as they have arisen in specific sectors, such as in relation to credit information,[143] financial

[143] *Fair Credit Reporting Act of 1971*, 15 USC § 1681 (1998).

institutions[144] and video rentals.[145] Data processing in the private sector is therefore largely left to be regulated by the market, or by industry self-regulation, rather than by law.[146]

In Europe, on the other hand, data protection is regarded as a fundamental human right. Legal protection of information privacy is seen as a necessary condition for citizenship, as well as being necessary for the development of a desirable society. Rather than taking individuals as they are, the European approach views social cohesion as premised on laws that guarantee rights. In explaining the contrast with the American approach, Reidenberg has characterised what he refers to as European 'social protection' norms in the following way:

> Under this governance philosophy, public liberty derives from the community of individuals and law is the fundamental basis to pursue norms of social and citizen protection. This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop, and information practices must serve individual identity. Citizen autonomy, in this view, effectively depends on a backdrop of legal rights.[147]

Rather than negatively protecting the ability of individuals to order their lives as they think fit, the European approach views rights as constitutive of the ability of individual citizens to participate in society.

The contrast is deep-seated. On the one hand, the American approach takes autonomous individuals as given, and conceives the role of the law as one of setting limits on government in order to secure pre-existing individual autonomy. On the other hand, the European approach regards individual autonomy as being only fully realised in society, and conceives an important role for the law in creating the conditions for autonomous individuals as participating members of a community.[148]

144 *Gramm-Leach-Bliley Act of 1999*, 15 USC § 6801 (1998).

145 *Video Privacy Protection Act of 1988*, 18 USC § 2710 (2000).

146 See, eg, Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace', above n 121, 1343.

147 Ibid 1347 (citations omitted).

148 The two approaches reflect a central dichotomy of liberal political theory, which Barry Hindess has explained as follows:

> The difference is a function of the ambiguity of the notion of autonomy itself — that is, of the central defining trope of the liberal project. In one case the focus is on the 'natural' status of human autonomy, and therefore on behaviour that is subject to no involuntary constraint. In the other case the focus is on the 'artefactual' status of autonomy, and therefore on the conditions under which it may be created.

Barry Hindess, 'Liberalism, Socialism and Democracy: Variations on a Governmental Theme' in Andrew Barry, Thomas Osborne and Nikolas Rose (eds), *Foucault and Political Reason: Liberalism, Neo-Liberalism and Rationalities of Government* (1996) 65, 76.

The European approach is clearly seen in the values underpinning German constitutionalism, which Donald Kommers has explained in the following terms:

> The German view, at bottom a Kantian moral perspective, finds the real meaning of liberty in community not apart from community. It does not identify autonomy with mere freedom of choice. To associate liberty with mere choice or atomistic individualism is to misunderstand the very nature of personhood.

Donald Kommers, 'German Constitutionalism: A Prolegomenon' (1991) 40 *Emory Law Journal* 837, 873 (emphasis omitted).

B *Understanding the Legal Sources of the European Approach to Data Protection*

Given the relatively conceptual approach taken to data protection in Europe, it is important for those from different legal cultures to examine the sources of the European approach in greater detail. The European approach can be seen as an essential element in the ambitious project of building a new, transnational law-based polity designed to prevent the disasters of the mid-20th century. In relation to data protection, the general approach is reflected in the requirement for EU member states to enact comprehensive data protection laws pursuant to the 1995 *Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data*.[149] The Data Protection Directive, which established new benchmarks for the protection of personal data of EU citizens, should be seen as building upon developments in information privacy laws in EU member states.

The single most important national development in this respect was the decision of the German Constitutional Court in the 1983 *Census* case, which recognised a 'right to informational self-determination'.[150] The *Census* case concerned the federal *Census Act of 1983*,[151] which required the collection of detailed information, including information concerning the use of transportation services and of public utilities, for social planning purposes, and allowed the information to be shared with local government authorities. The Constitutional Court held that, in certain respects, the legislation infringed provisions of the German *Basic Law* (*Grundgesetz*), namely art 1(1), which establishes the central constitutional value of human dignity, and art 2(1), which protects personality rights, including the right to free development of the personality.[152]

In recognition of the need for fundamental constitutional values to adapt to technological change, namely the development of data processing, the German Constitutional Court 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'.[153] The decision represented a recognition that the preservation of human dignity and individual autonomy, which are recognised as fundamental constitutional values, required a degree of individual control over

149 *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 281/31 ('Data Protection Directive').

150 65 BVerfGE 1 (1983).

151 *Volkszählungsgesetz*, v 25.3.1982, BGBl I S 369.

152 Article 1(1) of the German *Basic Law* states that: 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority'. Article 2(1) provides that: 'Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law'.

153 65 BVerfGE 1, 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): see Edward Eberle, 'Human Dignity, Privacy, and Personality in German and American Constitutional Law' [1997] *Utah Law Review* 963, 1002. All English translations of German cases are from Eberle, unless otherwise stated.

data processing.[154] In this respect, the Constitutional 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.'[155]

The decision also recognised that complete loss of control of personal data could inhibit individuals from exercising other fundamental rights, including the rights of assembly and freedom of expression. At the same time, to the extent that the exercise of fundamental rights is premised on the existence of a community, the Constitutional Court held that the 'right to informational self-determination' could be limited in the event of an overriding public interest. Thus, the Court acknowledged that it was permissible for census information to be collected for social planning purposes, but only on the condition that adequate safeguards were in place, including safeguards to ensure the anonymity of respondents.[156] The *Census Act of 1983* was therefore required to be amended in order to ensure that the necessary safeguards were put in place.

The 'right to informational self-determination' is an attempt to apply the fundamental German constitutional concepts of respect for human dignity and individual autonomy to the context of data processing. Given the Kantian understanding of autonomy as self-determination within a law-based community, this entails more than the imposition of negative limits on data processing activities — it also includes the positive ability of individual data subjects to participate in decisions relating to data processing. Moreover, these participation rights were conceived as extending to all stages of data processing, encompassing collection, use, storage and disclosure of personal information.[157] Following the German Constitutional Court's decision, individual rights to participate in data processing were recognised in a number of national laws of European states, including Germany, Norway, Austria and Finland, in the late 1980s and early 1990s.[158]

Nevertheless, reliance on individual participation rights within the concept of the 'right to informational self-determination' was, in practice, found to provide inadequate protection for individuals, mainly because of the power imbalance between data processors and individual data subjects. This meant that individuals would commonly fail to exercise their rights to participate in data processing, or that those rights would be readily bargained away. The result of this experience was the development in the 1990s of European approaches that built upon participation rights, while attempting to provide greater protection for individual

154 As Eberle explains, '[a]t 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': Eberle, above n 153, 1004.

155 *Census*, 65 BVerfGE 1, 43 (1983): ibid 1002.

156 *Census*, 65 BVerfGE 1, 43–4 (1983).

157 Thus, Mayer-Schönberger explains that pursuant to the right to informational self-determination, '[t]he individual cannot only … once and for all decide in an "all or nothing" choice to have his or her personal data processed, but has to be — at least in principle — continuously involved in the data processing': Mayer-Schönberger, above n 99, 229–30.

158 Ibid 231–2.

data subjects — including greater protection for 'sensitive' personal information and sectoral-specific laws, such as those applying to health information.

The historical evolution of national European data protection laws provides the essential background to understanding the 1995 Data Protection Directive. The development of the Data Protection Directive must also be seen within the context of the transformation of the EU from a purely economic union into a political union.[159] As a matter of European law, the Data Protection Directive rests on the necessity of removing differences in order to promote the free flow of personal information to better achieve an Internal Market.[160] As Spiros Simitis explains, however, the transition into a political union, while not compelling the adoption of a data protection directive, effectively meant that any such directive would approach the regulation of data processing from within the framework of fundamental rights and freedoms, thereby establishing a 'high level' of protection of personal data.[161]

The rights-based approach to data protection is evident in both the recitals to the Data Protection Directive and in its substantive articles. The importance of this framework in establishing a 'high level' of protection is seen most clearly in recital 10, which provides 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, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; 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.[162]

The historical development of the specifically European approach to data protection may be seen in a number of central features of the Data Protection Directive. First, the Data Protection Directive applies minimum principles to all stages of data processing, generally not distinguishing between collection, storage, use or disclosure.[163] Secondly, a rights-based approach to data protection is found throughout the Data Protection Directive including, for example, articles that provide for rights of access and rectification,[164] and rights to object to the

159 *Treaty Establishing the European Economic Community*, opened for signature 25 March 1957, 298 UNTS 11, art 146 (entered into force 1 January 1958), as amended by *Treaty on European Union*, opened for signature 7 February 1992, [1992] OJ C 191, 1, art G (entered into force 1 November 1993).

160 As the *First Report on the Implementation of the Data Protection Directive* notes:

> In legal terms … the existence of the Directive rests on Internal Market grounds. Legislation at the EU level was justified because differences in the way that Member States approached this issue impeded the free flow of personal data between the Member States. Its legal base was thus art 100a (now art 95) of the Treaty.

Commission of the European Communities, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, Doc No COM (2003) 265 final (2003) 3 (citations omitted).

161 Spiros Simitis, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data' (1995) 80 *Iowa Law Review* 445, 447–8.

162 Data Protection Directive, recital 10.

163 See, eg, Data Protection Directive, arts 6–7.

164 Data Protection Directive, art 12.

processing of personal data for the purposes of direct marketing.[165] Thirdly, the Data Protection Directive allows, in certain instances, for mandatory standards of protection that cannot be contracted out of by data subjects. For example, under art 8(1), sensitive personal data, including data concerning race, political opinion or religious belief, generally cannot be subject to data processing. Although provision is made for the processing of sensitive data with the consent of the data subject, the ability of member states to prohibit processing of such data even with consent is expressly preserved.[166] Moreover, the requirements for consent under the Data Protection Directive are quite rigorous. Article 2(h) defines the 'data subject's consent' as being 'any 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.'[167]

Despite the political compromises that were necessary in the process of formulating the Data Protection Directive, it is clear that it establishes a new, much higher, level of protection of personal information than the broad standards set in the earlier period of convergence of data processing approaches.

Moreover, the Data Protection Directive is consciously designed to promote international convergence at this higher level of protection. Given the transborder nature of data processing, it was considered necessary to establish a mechanism to ensure that the personal data of EU citizens was protected in the event that it was transferred outside the borders of member states. This mechanism, established pursuant to ch IV of the Data Protection Directive, essentially requires member states to prohibit the transfer of personal data to third countries where the third country fails to ensure an 'adequate' level of protection for the data.[168] The threat of a 'data embargo' has provided the basis for the EU to enter into negotiations with third countries, with a view to ensuring a level of protection consistent with the European rights-based approach.

C *Understanding the Sources of American Differences with Europe and the 'Safe Harbor' Compromise*

While EU member states, both individually and collectively, were refining a rights-based approach to data protection, information privacy policy in the United States proceeded in a different direction. Since the Reagan administration, United States economic policy has largely been characterised by a neo-liberal belief in the primacy of the market, and a corresponding commitment to 'deregulation' and minimum intervention in market processes. This pro-market orientation has also characterised American information privacy laws which, apart from

165 Data Protection Directive, art 14(b).

166 Data Protection Directive, art 8(2)(a).

167 Data Protection Directive, art 2(h).

168 Thus, Data Protection Directive, art 25(1) states that '[t]he Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if … the third country in question ensures an adequate level of protection.' Schwartz refers to the ability to block international transfers of personal data as a 'data embargo order': Paul Schwartz, 'European Data Protection Law and Restriction on International Data Flows' (1995) 80 *Iowa Law Review* 471, 488–92.

the introduction of sector-specific laws, have remained frozen since the formulation of the fair information practices in the 1970s.[169]

With the growth in the commercial use of the internet from the mid-1990s, the neo-liberal suspicion of government regulation combined with the liberal First Amendment commitment to the free flow of information, reinforced the American preference for private sector solutions to information privacy. Thus, in response to the requirement under the EU Data Protection Directive that third countries provide 'adequate' protection, the United States claimed that industry self-regulation was capable of satisfying the Directive's standards. The 1997 Clinton–Gore policy statement, entitled *A Framework for Global Electronic Commerce*, for example, included the following response to the EU Data Protection Directive:

> To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled.[170]

With the commencement of the Data Protection Directive on 25 October 1998, the incompatible approaches to the protection of personal information created tensions between the EU and the United States. The requirement under the Data Protection Directive that third countries provide 'adequate' protection to the personal data of EU citizens brought these tensions to a head. The EU saw the 'adequacy' requirement as a means for pressing the United States to adopt comprehensive data protection laws.[171]

At the same time, it was inconceivable for either the EU member states or the United States to contemplate the commercial consequences of an interruption in data flows between Europe and the United States. To prevent this from happening, the United States Department of Commerce and the EU entered into consultations with a view to developing a compromise. The negotiations proved to be difficult, with the EU rejecting five proposals submitted by the Department of Commerce over a two year period before the parties were able to reach an agreement.[172]

169 Writing in the early 1990s, Gellman stated that '[t]he election of Ronald Reagan as President marked the end of any significant privacy policy initiatives from the executive branch. This resulted in a divergence between the United States and other western industrialized countries on privacy matters': Gellman, 'Fragmented, Incomplete, and Discontinuous', above n 97, 202 (citations omitted).

170 William Clinton and Albert Gore Jr, *A Framework for Global Electronic Commerce* (1997) [II.5].

171 Mike Ewing, for example, explains that '[a]s the Data Protection Directive neared implementation in 1998, the European Union began to pressure the United States into adopting either the Directive or its own comprehensive data protection scheme': Mike Ewing, 'The Perfect Storm: The Safe Harbor and the Directive on Data Protection' (2002) 24 *Houston Journal of International Law* 315, 336.

172 See, eg, Gregory Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards' (2000) 25 *Yale Journal of International Law* 1; Joel Reidenberg, 'E-Commerce and Trans-Atlantic Privacy' (2001) 38 *Houston Law Review* 717; David Castor, 'Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year' (2002) 12 *Indiana International and Comparative Law Review* 265.

In March 2000, the EU and the United States Department of Commerce eventually reached agreement on a set of seven voluntary principles, known as the 'Safe Harbor Principles'. The Safe Harbor Principles were issued by the Department of Commerce on 21 July 2000,[173] and together with a set of frequently asked questions ('FAQs'), received the official approval of the European Commission as satisfying the 'adequacy' requirement under art 25 of the Data Protection Directive on 26 July 2000.[174] Following from the United States' policy commitment to self-regulation, the Safe Harbor Principles are not mandatory, but apply only to private firms that subscribe to the principles.[175]

Despite the extent to which EU policy documents make it clear that the 'adequacy' requirement is intended to promote a higher level of protection than the baseline OECD Guidelines,[176] it is clear that the Safe Harbor Principles go no further than the Guidelines. Mike Ewing has commented that:

> The Safe Harbor Principles do not match the breadth and depth of the Data Protection Directive. They replace the Directive's principles of limited collection and use as a fundamental right with an opt-out provision; the data subject is granted a lower degree of control over his personal data. The opt-in provision for sensitive data is weakened by limits on the provision of an opt-in choice for certain categories of sensitive data. … Compared with the broad rights of access granted by the Directive in art 11, the access rights promulgated by the Safe Harbor fall short.[177]

The Safe Harbor compromise, therefore, effectively preserves the fundamental differences between the European and American approaches. Insofar as it represents a concession to the American preference for the free flow of information it can, moreover, be regarded as reinforcing impersonal, market-based processes at the expense of European views of autonomy and dignity.

VII THE FORUM OR THE MARKET: WHAT IS AT STAKE IN THE CONFLICT BETWEEN EUROPE AND AMERICA?

For a jurisdiction such as Australia, which is currently engaged in the process of developing privacy and information privacy laws, it is important to understand what is at stake in the different approaches to privacy in Europe and in America. Assistance in this task can be found in James Whitman's recent analysis of the 'two Western cultures of privacy'.[178]

173 United States Department of Commerce, *Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 Fed Reg 45666 (2000).

174 *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce* [2000] OJ L 215/7.

175 *FAQ 6 — Self-Certification* in United States Department of Commerce, *Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 Fed Reg 45666, 45669–70 (2000).

176 See, eg, Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, adopted 24 July 1998, Doc No DG XV D/5025/98 WP 12 (1998).

177 Ewing, above n 171, 341–2 (citations omitted).

178 See James Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151.

According to Whitman, the two approaches reflect two aspects of privacy which are related to different understandings of 'personhood'. Thus, Whitman characterises Continental European privacy rights as 'at their core, a form of protection of a right to respect and personal dignity'.[179] He traces the origins of the European approach to traditional concerns with protecting personal honour in hierarchical European societies. While the honour of members of the aristocracy had traditionally been protected by social norms regulating insults and by duelling, the 19th century saw the replacement of duelling with legal protections, and the beginning of a 'levelling up' of the protection of honour, which eventually became available to all members of society. Conversely, Whitman characterises the 'conceptual core' of the American approach as 'the right to freedom from intrusions by the state, especially in one's own home'.[180] In this sense, the essential approach of American privacy law has changed very little since the 18th century.

While Whitman's historical analysis is informative, it is more important to grasp the essential features of the fundamentally different orientations of the European and American traditions. The best way to do this is by reference to their respective attitudes to the market. Basically, the American approach seeks to promote consumer-based choice through market mechanisms, whereas the European approach sees the market as a threat to human dignity. As Whitman expresses this contrast:

> Europeans have a harder time seeing the benefits of free-market solutions … Privacy is an aspect of personal dignity within the continental tradition, and personal dignity is never satisfactorily safeguarded by market mechanisms … As one French scholar insists, contrasting the American attitude with the French, one can freely dispose of one's liberty, but one can never be permitted to freely dispose of one's dignity. If one accepts that premise, one should accept the proposition that any consumer's consent to the sale of his or her data should have only limited effect at best.[181]

From this perspective, then, it is clear that the fundamental choice in developing all forms of privacy law, but especially information privacy laws, lies between a consequentialist or market-based approach, and a deontological or rights-based approach.

VIII CONCLUSION

Australian privacy law now faces fundamental choices concerning the protection of privacy, both at general law and in relation to information privacy laws. This article argues that the choices should be made on the basis of a principled approach to the concept of privacy, and with an understanding of the important divergence between the two main post-Enlightenment philosophical and legal traditions: that of Europe and America. This article further claims that decisions about the shape of privacy laws should take into account the two main

[179] Ibid 1161 (emphasis omitted).
[180] Ibid.
[181] Ibid 1193.

Enlightenment-based strands of moral and political thought that have been applied to privacy theory, namely deontological and consequentialist approaches. While no legal and political system is a pure example of either approach, the American approach is clearly more welfare-consequentialist and the European approach more Kantian-deontological. The differences can be clearly seen in the fundamental orientation of the two legal systems towards the market: the American approach tends to see the law as secondary to market processes, while the European approach seeks to preserve autonomy and dignity from perceived threats of unconstrained market processes.

The choice between consequentialist and deontological approaches should shape both general law protection of privacy and information privacy laws. First, in relation to the development of privacy protection at general law, difficult questions arise concerning the role of rights in the development of private law, especially in common law jurisdictions. In the United Kingdom, for example, following the introduction of the *Human Rights Act 1998* (UK) c 42, there is a continual tension between Continental rights-based jurisprudence and the incremental processes of the common law. This tension is now embedded within the parameters of the action for breach of confidence. As far as potential Australian developments are concerned, it is important to appreciate that the choice between a consequentialist, interest-based approach and a deontological, rights-based approach is not straightforwardly related to the choice between developing the action for breach of confidence and recognising a privacy tort. Whichever path is adopted, an interest-based approach would lead to less protection — and perhaps no specific protection for privacy — than a rights-based approach. At the very least, the approach adopted would have implications for the degree of protection at general law, including matters such as defences and remedies.

Secondly, in relation to information privacy law, the implementation of the EU Data Protection Directive has exposed considerable tensions between the EU and Australia in the underlying approaches adopted towards data processing. This article contends that the concerns expressed regarding the 'adequacy' of the Australian laws by the EU Working Party[182] need to be understood in the context of the conceptual foundations of European data protection law. In other words, the European rights-based approach necessarily confers a higher level of protection on data subjects than a market-based law. For example, a rights-based approach would require more explicit and informed consent to data processing than a welfarist approach, which might consider that, in certain circumstances, implied consent is acceptable. Moreover, in some situations, a rights-based approach might consider that protecting the autonomy and dignity of data subjects would require the prohibition of forms of data processing, regardless of the consent of the data subject. Similarly, the kinds of information falling within the scope of information privacy laws would likely be much greater under a rights-based approach than under a market-based approach. Finally, the extent to which data protection principles can be expressed in 'technologically-neutral'

[182] Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, adopted on 26 January 2001, Doc No 5095/00/EN WP40 final, art 29.

terminology may differ, depending upon the approach adopted. In other words, a rights-based approach might wish to regulate particularly intrusive forms of data processing, thereby shaping technologies, whereas a consequentialist approach may be more inclined to allow technological developments to be determined by the market. All of these issues merit future detailed analysis.

Although the future shape of privacy law must reflect either a consequentialist or deontological approach, an essential argument made in this article is that the concept of privacy should be interpreted in the context of progressive micro-political struggles over individual identity which occur within overall social processes of rationalisation and normalisation. From this perspective, Enlightenment-sourced consequentialist and deontological approaches are both implicated in the progressive rationalisation and normalisation of society. On the one hand, welfare consequentialism tends to reduce individuals to consumers who are incorporated in impersonal market-based processes. Traditional rights-based approaches, on the other hand, adhere to a formalistic, universalising concept of the self, which entrenches particular views of the individual as atomistic, self-determining and rational. To this extent, deontological approaches to privacy are also normalising. Despite this, a rights-based approach presents considerably more space for struggles over individual identity, including debates over forms of subjectivity, than does welfare consequentialism. In other words, a rights-based approach may present a bulwark, or 'speed bump', in the face of the seemingly inexorable advance of global market forces.[183] Especially in a largely consequentialist society such as Australia, a rights-based legal approach to privacy should be seriously considered as a means of promoting more pluralistic approaches to identity, and of resisting global normalisation and homogenisation.

[183] In this context, Jeffrey Rosen has expressed the concern that 'as Europe becomes more and more like America — that is, more market driven, less hierarchical, more democratic, and more distant from its aristocratic past — the popular consensus about the importance of protecting dignity will atrophy and eventually collapse under the weight of market forces': Jeffrey Rosen, 'Continental Divide' (September–October 2004) *Legal Affairs* <http://www.legalaffairs.org/issues/September-October-2004/review_rosen_sepoct04.html>.