# Privacy and Technology: a Problem of Regulation and Rights

## Introduction

The ubiquitousness of privacy issues, and the risks that they pose, in the world of business, has been highlighted by a recent Congressional investigation, which has seen members of the board of Hewlett-Packard (HP) resign, and the prospect of criminal charges being laid. The issue at the heart of this imbroglio is the use of "pretexting" – using false identities – and using tracing technology embedded in emails to access telephone records of employees, directors and journalists and to investigate their linkages.[1]

In developed western nations there has been a longstanding interest in privacy, an interest which is almost woven into the fabric of society. A simple example of this embeddedness is the aphorism that 'an Englishman's home is his castle'. In the last decade this interest in privacy has intensified and is being applied to an increasing number of areas, frequently in the phrase 'right to privacy'. As far as I can see the concept of privacy has achieved little purchase in much of Asia where there is less of a tradition of individualism or individual rights. Nevertheless, with increasing affluence and technological sophistication it likely that there will be a growing interest in privacy. This concern will not be confined to organisations of a particular size or in a particular sector. Indeed, it is a key contention of this paper that the issue of privacy is or will become important to employees, owners and managers of SMEs.

Privacy rights risk becoming a 'wicked problem'[2] – an intractable contest between rights claims and technology: definitions of key terms such as 'privacy' are not agreed upon, whether there is a problem is contested, and widely varying solutions may be unsuccessful, add to the problem, or create a new and worse problem. This risk is particularly important in two areas: information collection and distribution and workplace surveillance.

Technology changes traditional confidentiality of records, advice, deliberation and work; it encourages new forms of information management, openness and

also secrecy.[3] While it therefore enlarges the scope of government capacity to obtain, store, use and distribute data on citizens, it also alters patterns of work and builds new demands for accountability. Thus it can be seen that privacy has shifted from its earlier focus on concerns around bodily, intimate and physical protection, the private sphere of life, to concerns about invasions of informational and decisional privacy and modern surveillance techniques.[4]

In the workplace, surveillance has a key role in monitoring safety and compliance with laws on harassment or bullying, such as might occur via email and SMS (mobile telephone) systems, but it also has a role in monitoring efficiency.[5] It can provide management with insight into misuse of resources, including data. In one recent instance, the main employment agency in Australia announced a raft of dismissals, resignations and further investigation of employees discovered to have accessed data improperly, used or distributed that data improperly, and in some cases to have falsified it. Technical capacity to detect such behaviour raises questions of values and of individual privacy but also provides reassurance that some other privacy has been protected.

Privacy, then, is core issue for Information and Communication Technology (ICT) for work and in workplaces.

**What is privacy?**

What is the content of the word 'privacy', how the state should respond to it – if at all – and whether it is a problem of rights, or some other kind of problem, are difficult questions.

Commentators often use 'privacy' as though it has a precise meaning, but in fact it depends on specific cultural or political values. When we seek to define privacy with reference to experience in other countries, each with their own traditions and institutions, we soon detect diversity . The United States, for example, tends to favour the rights of capital over the rights of labour, and it worries less about effects on privacy; surveillance of communications is a fact of life.[6] French law,

by contrast, favours the view that people enter the workplace with private rights intact and any infringement must be strictly necessary and for specific ends.[7] Australian employers tend to tolerate a certain amount of non-business communication, but there is no right to such tolerance.[8]

The Victorian Law Reform Commission has put the problem succinctly: 'privacy is a slippery term for which there is no adequate legal definition', but 'legal theory must nevertheless attempt to come to terms with the problem of privacy, and find ways of determining how the law can best regulate those values that are mobilised in the name of privacy'.[9]

**A right to privacy?**

Privacy as a right is traced back to *The Right to Privacy* by Warren and Brandeis who in 1890 defined privacy as an individual right 'to be let alone'. This traditional liberal perspective is embedded in US approaches to government: it restricts government power through negative controls.[10] Warren and Brandeis argued that solitude and privacy have become essential because of the increasing intensity and complexity of life, and – in an early awareness of technical capacity – the intrusiveness of journalism.[11] They distinguished privacy from legal actions such as slander and libel, which were presented as forms of intangible property rights. They posited privacy as a right in itself, premised upon the principle of 'an inviolate personality'.[12] But this conception of privacy as a right is at odds with other legal handling of damages to people. According to Leebron, 'part of the legacy of Warren and Brandeis is that the privacy tort is virtually the only tort' conceived of as a 'right, rather than the more familiar concept of a tort as the conduct of the defendant or the consequential damages suffered by the plaintiff'.[13]

Commentators who embrace 'privacy as a right' connect privacy to concepts of personal autonomy and identity, and to human rights ideas relating to the inherent dignity of the person.[14] This is generally theorised in connection with the private sphere of life and personal relationships.[15] A second theme is about

controlling personal information and restricting access to the self. This strongly overlaps with the first, but also addresses concerns about new technologies and their potential to reveal personal information about individuals. Often the two themes are linked together.[16]

Another approach is 'pragmatic' or 'functionalist'. This largely rejects concerns about 'rights' or 'values', and instead focuses on the 'interests' or 'practices' needing protection under the rubric of privacy. Privacy is valued instrumentally, and in contrast to the rights approach, is also valued contextually.[17]

For government, the crucial interest at present may well be informational privacy.[18] Government needs to provide a legal framework that protects individual privacy, yet also permits effective, authorised data gathering by its own agencies and by employers.[19] Such data are necessary for informational and for enforcement purposes. But informational privacy does not address issues like surveillance, monitoring, testing and searching, or the dynamics of workplace power relations in which invasions of privacy occur, or bodily, territorial or communication interests.[20] Second, attempting to define privacy based on *interests* can move it closer to an economic approach in which privacy is a marketable commodity.[21] This shifts power from individuals to corporations. Certainly individuals could trade their privacy, and be paid for the information they furnish,[22] but in dealing with both business and government, disparity of power is obvious.[23] Privacy and power are interconnected, particularly in the workplace, where practices such as monitoring workplace email are part of a continuum that includes surveillance cameras in the workers' changing rooms, random drug testing and so on.[24]

The issue of privacy protection did not become a concern in Australia until 1985 when the Australian government attempted to address serious tax evasion through the development of a national identification scheme. The 'Australia Card' proposal involved a central register containing data about each resident. What was proposed was an obligatory, multi-purpose identification card, which would have been required in order for citizens to deal with government agencies and

private sector organisations, such as employers and financial institutions. Equivalent obligations were to be placed on organisations to demand the card and record its code. The proposal generated wide public concern about intrusions into citizens' privacy and also record keeping on individuals. It was opposed by various civil liberties bodies, and prompted the creation of the Australian Privacy Foundation. As a result of public opposition, the Bill failed to pass the Senate and was replaced by a more modest proposal that created a single purpose tax file number for all working age citizens.[25] Ironically, the chief political opponents of the card – Prime Minister John Howard and Attorney General Philip Ruddock – are now in government, and are proposing, as a response to threats of terrorism, a similar scheme to the Australia Card, but containing additional technical advances. With its growing interest in general intrusiveness on security grounds, government information gathering may also spill over into workplace surveillance – witness the controversies about government direction of research into terrorism in universities.[26]

**Is a definition of privacy necessary?**

A precise definition of privacy remains elusive, and this places severe limits on the range of government responses. But it is not necessary to have a precise definition as is evident from the European adoption of a 'floor of rights' approach. The 'floor of rights' approach has been applied successfully across both public and private spheres of power, and has been able to address private spheres of life as well as relationships of power, as found in the employment relationship.[27] The European Union approach also shows the importance of building a comprehensive and integrated approach. A privacy regime that protects workers' rights is anchored in a longstanding, broader, progressive, 'rights culture', where the notion of the 'human rights of workers' is already part of the political or philosophical lexicon.[28] The existence of an array of instruments, codes, and conventions governing broader arrangements of power in society, between citizens and government, citizens and the legal system, and between citizen and

citizen also provides a frame within which the privacy discourse is undertaken and in which government policy is implemented.[29]

Thus, the broader sociopolitical framework has implications for the governance of workplace privacy and of privacy generally. Building a privacy regime in a vacuum is likely to prove problematic and result in divergent outcomes.[30]This conclusion has significant implications for the development of a comprehensive privacy protection regime.

**Enter technology**

Information and communication technology (ICT) offers enormous potential for the surveillance of citizens. Closed circuit television in public places and business premises, iris scanners at airports, facial recognition technology, electronic freeway tolling, the deployment of traffic cameras, and information supplied to internet servers by the use of customers' credit cards, can track, monitor and provide a massive amount of personal information.[31] On a Weberian-Orwellian view, the extension of surveillance is part of a broader social movement that aims at control.[32] In the workplace, this becomes surveillance of workers to ensure compliance with rules. From a Foucaldian perspective, surveillance is a technical example of the Panoptic lens, which ensures that all workers can be watched and they cannot know whether they are being observed at any one time.[33] Taylorist management perspectives see such surveillance as the natural development of scientific management.[34] At a societal level, CCTV, mobile telephone tracking, improved satellite visual tracking and a range of implanted technologies in equipment and in people themselves can ensure a high level of monitoring. One side of this argument would be that such monitoring allows for improved planning (for example, traffic patterns, transport use, congestion in public spaces); the other side would be the risk of assembling data sets to establish patterns of movement that support inferences of illegal intent.

The intrusiveness of technologies is apparent in the surveillance of email, voice mail and internet 'surfing', the monitoring of keyboard strokes, the introduction of

biometric ID systems, alcohol and drug testing, genetic testing and pre-employment investigations. The tools upon which many employees work are themselves the objects of surveillance, and they can be checked without the operator's knowledge.[35] Concerns about privacy and surveillance bring to the fore requirements that are placed upon organisations and managers which may conflict with individual privacy rights. Effective management of these issues is one of the major challenges facing business, particularly as new technologies open up greater possibilities for data-sharing and other forms of networked collaborative working. Not dealing with these competing issues risks forfeiting the opportunities that ICT offers by imposing inappropriate controls or, conversely, failing to take advantage of benefits for efficiency and proper behaviour.

The management of workplace privacy can be further complicated by issues that are unrelated to technology but which require employers to balance the necessity to regulate behaviour and protect privacy. For example, in the Australian context one highly problematic scenario involves workplace relationships and the potential for co-worker dating to result in allegations of sexual harassment.. Thus, on the one hand, employment rules concerning relationships between co-workers may be an invasion of privacy, but, in the absence of such rules, organisations may expose themselves to liability under equal opportunity or occupational health and safety legislation.[36].

**To regulate or not?**

ICT and regulation of privacy are thus enmeshed in shifting webs of problems and proposed solutions. The more we know about technology the more insoluble issues of privacy threaten to become. Regulation to protect privacy has emerged as a strongly supported 'solution' for a 'problem of privacy'.[37]

Regulation is in fact peculiarly unsuited for ordering ICT activities, because it seeks to organize a constantly changing space in which the patterns are unknowable. Regulation, too, is only desirable when it benefits society over and above any costs it imposes. We should therefore explore whether regulation's

costs (constraints on ICT opportunities and benefits) outweigh gains (perceived individual privacy).

In business, restricting the organization's 'right to know' the ways in which employees are using the email or telephone systems is partly an issue of ensuring privacy in personal communications (if that is permitted in any case), but it comes up against risks of reckless behaviour that may jeopardize the business or the deliberate transfer of intellectual property to an external recipient for personal gain.

For government, too, preoccupation with individual privacy, for example, is often at odds with demands for information or services.[38] Citizens often cannot articulate their concepts of privacy, but they 'know privacy when they see it'.[39] They have contradictory attitudes towards data-sharing:[40] for example, they approve of data sharing to attack terrorism or violent crime, but not to uncover tax or welfare fraud.[41] They do not easily separate privacy concerns from service demands. Moreover, we notice loss of privacy when attention is drawn to it, but not otherwise, yet in the ICT world, exchange between the individual and the wider domain of transactions and information gathering and sharing is constant and expanding.[42] What people think privacy is, and whether they are passionate about it, depends on who asks, what is asked, and the context of the request.

In debates about privacy two types of public interest collide, one interest in individual identity and security confronts another of demand for services and security. The general public interest, often directed at public goods like health that depend on substantial data and sharing that data, comes up against privacy as a private good that seeks to withhold release or release selectively. Conceptually, this latter privacy is restrictive and reactive; the inside (the self) maintains barriers against pressure from the outside (the other).[43] Yet regulation supporting such privacy depends heavily on the 'outside', the legislative and administrative power of the state, and requires a positive engagement of the state in the support of citizens' interests. Consequently it can be argued that the citizens' interests or rights in privacy may be subordinated to a greater public

interest.

There is a need for deeper examination of the implications of ICT for privacy. ICT effects are mercurial – but also fungible, hard to confine. Technology generates secure systems *and* attacks on them simultaneously with regimes that deter, punish and remediate; corrective aspects include systems that warn of likely infringements (for example, in accessing pornographic or other criminal sites), systems that remove access because of infringements or report them to authorities, and, of course, algorithms designed to counter misuse, viruses, etc.[44] The skills deployed to create secure transactions are the same as those used to 'break' that security, while the legal system uses its efforts to deal with such breaches, even while creation and counter-attack are occurring. The result is that capacity for protecting and revealing information is constantly changing in extent and nature, because that is inherent in the technology, but law struggles to address such a fluid situation. What constitutes privacy at this juncture may not therefore be the same privacy within a few years or even months, because of technological advances:[45] Each advance poses a different challenge that requires integration into the privacy debate. ICT-mediated conversations, written or oral, telephonic or via computer, are embedded in several layers of revealing data, depending on the style of communication (email versus telephone, for instance). Adding a real-time, camera capacity enhances communication, but also reveals expression and body language (which may run against the tone of voice) and may reveal other listeners, background information, location, and so on, which the speaker(s) might wish to remain 'private', even from one another. Technology also branches out into unexpected disciplines, interests and questions;[46] it does not behave in a linear fashion that encourages predictability.[47] Privacy, then, can seem to emerge as a function of technical capacity, not a right or capacity of a fixed, unchanging kind.

**What does the law do and can it really do it?**

Regulation generates as well as redresses complaints about privacy breaches

through raising awareness.[48] Laws defining 'sensitive information' also skew attention towards areas that often do not excite citizen attention: ethnicity, sexual orientation, religion, politics and lifestyle appear of little concern compared with addresses and finance, *unless respondents are prompted*.[49] Law therefore in part creates the 'problem of privacy' by identifying behaviours deemed to breach it. The five-yearly census in Australia in 2006 briefly excited such interest, with a range of objections to revealing 'private' information, even though identification was to be removed and strict legal guarantees of protection were imposed.[50]

Law also appears ignorant of ICT's shifting capacities. Law relies on its resistance to speed to assure interpretive certainty. But when ICT influences law through changes to language and methodology, it also influences the outcomes of law and alters law's territory: for example, legal reliance on paper documents and handwritten signatures is changed with ICT-generated documents (or 'virtual' documents) and electronic signatures that are complex digital algorithms, yet whose date and time, also embedded, is not always visible – what does this mean for a 'communication' or 'evidence'? Computer documents are not documents as we have understood them until they are printed (and therefore may also be digitally manipulated), because until then they take on a screen appearance that masks their digital nature. The law-ICT intersection between government capability, responsiveness to constituencies, electoral cycles, professional behaviour and technical possibility is a meeting of paradigms rather than an adjustment between competing methodologies and technical knowledge. Law's knowledge relies on historical data for extrapolation; ICT knowledge shows little interest in history as self-reflection or respect for precedent. Law relies on order as a condition and consequence of its function; ICT algorithms are precursors to exploration of unexpected possibilities – they provide a way forward that may be very different from the experience from which they emerge.[51] This means that law is constantly looking back to use experience to decide on present issues, constraining itself, while ICT, equally constantly, abandons its position to look forward, unconstrained by past lessons. ICT can therefore shift much faster in its behaviour and responses than law.

Regulation's *advantage* is that analysis, proposal, promotion, consultation and implementation fall within a bureaucratic paradigm, yet its reactive system, unable to anticipate ICT implications, threatens to stifle them, foreshadowing problems without offering solutions.

Because of changing problems and piecemeal responses, privacy laws are also subject to fragmentation[52] and may be latecomers among other regimes that affect privacy, such as Freedom of Information and Ombudsman's Acts, regimes governing professions, regimes managing taxation and health, or rules for reporting performance to government. Differentiation encourages a focus on specific issues that omnibus legislation cannot supply: comprehensive legislation to protect privacy as a universal right appears to be impossible, not only because of changing technology, as we have noted, but because of the range of 'privacies'. On the one hand, it can be assumed that there is a privacy protection, as a general condition, when there may not be (examples abound in government action and data sharing), and, on the other, as we have also seen, self-privation or restraint may prevent useful sharing (constraints on data sharing by the Australian Taxation Office through its unique Tax File Number system is an example).[53] A general set of privacy principles is similarly difficult to construct, and for the same reasons of changeability and lack of specificity. In federal systems like Australia's, parallel legislation at federal and state level is an additional load.[54]

These problems, then, are a consequence of three factors: the elusive character of privacy; the protean impacts of ICTs; and asking regulatory instruments to carry too heavy a burden. The problems posed by regulatory solutions can be in part resolved by shifting the frame to other institutional responses, which include law but also integrate it with broader considerations of public policy and management. This is not a way of disempowering citizens or of eroding rights but of moving toward a regime which is flexible, adaptive, and based on citizen engagement with those issues that are of concern.

Shifting the frame of reference can be helpful. The intractability of questions in

certain contexts can mask useful advances in data sharing and privacy analysis that seek to resolve obstacles to e-government.[55] Pragmatic initiatives include design of protective instruments that emphasize in-built safeguards rather than redress of complaints, 'soft' regulation and 'gentle' enforcement, rather than 'command-and-sanction'.[56] Such initiatives are part of a shift towards quasi-self-regulatory systems that rely more on education and exhortation than on central direction backed by penalties as a first or likely response.

The drivers for sharing and control move in contrary directions,[57] but when we grant government legitimacy in invading our privacy, we allow the means of that invasion to remain secret, acknowledging necessity but also practical limits to non-technical understanding. Certainly ICTs embody capabilities such as data-mining that enlarge intervention capacity. In principle, too, preferring security rather than private values uncomfortably evokes old state assertions of prerogative rights. The security debate, for example, bypasses rather than resolves competing demands of government (representing societal rights) and individuals (asserting private claims). It illustrates intersecting, paradoxical yet pragmatic policy responses linked to technology, and it signals the costs of failing to develop effective information sharing.

For governments like Australia's, the problem is in retaining final say in how or what communications they intercept, in not sharing all the technical secrets they have, while re-engaging people and organizations in government business and supporting social linkages. Because of cultural predispositions towards individual control, popular skepticism about the role and effectiveness of government (and, more broadly, issues about how much trust citizens do indeed repose in their governments), and a history of raising concerns about how government might use the information it collects, Australia is a particularly difficult case for managing privacy in an environment that demands greater levels of security. Although the current federal government now requires information and more secure systems, when in opposition it opposed such controls, and as a government it has been unwilling to press on too quickly even in matters such as health or taxation. It has not fully resolved its 'liberal' interest in freedom from

government with government need for information whose collection can imply intrusion. The government therefore applies its information gathering regimes inconsistently and in response to perceived political acceptance: national security justifies great intrusion; breaches of the tax law are not so serious; and data for health programs must get along without all desirable information.

Protection of privacy, like privacy itself, emerges as a function of technical possibility. How then do we avoid privacy obstructing progress in business and government yet also recognize social norms and furnish services?[58] We may change the behaviour and presentation of those collecting information, to transfer responsibility and control to information providers and users, to avoid paralysis in the face of opposition.[59] The policy problem is to create management regimes that do not forfeit technological benefits but also do not privilege them over all other considerations.

Management regimes recognize the extent to which the population will accept changed boundaries between the individual and society. Privacy regimes must delineate territories with permeable, shifting borders to accommodate unpredictable ICT capacity. Privacy regimes set the operating framework within which management must function, but with one eye to feasibility. Governments will have to ask citizens what data belong to individuals and what might be shared with employers, business or government. Information most obviously private is also information usefully shared, such as in health. Governments can then use technology to reinforce and manage service and data privacy.[60] Exploration of the ways forward is at an early stage. Governments, for example, clearly have to build and rebuild trust with citizens.[61] They may have to assist more actively in distributing and accessing ICT but also provide education in support. They will have to demonstrate that the exchange of information between government and citizens is principally in the citizens' interest. They will have to show, conclusively, that more efficient, effective and people-friendly services follow from this exchange. One strategy not explored here is deliberative polling.[62] Individual privacy protection is as much an issue for political decision and public policy as for law or technical capacity.[63] In plain terms, this suggests

the desirability of asking citizens what they want as a first step, not as an afterthought.

**Where to next?**

Privacy can be understood not as a special problem but as a domain around which issues of engagement between people and their systems cluster. People engage, on varying, often unequal terms, with government, with business, with technology, with civil society at large, and with individuals. All these links bring with them elements of privacy, but not the same elements or the same mix of elements in each case. Privacy policy may appear different from other policy sectors because of the newness of technical facades, but the useful means of address are the old, tried ones. Privacy is but one issue of governance and management.

An approach drawing on the fields of public policy and management suggests integration strategies designed to generate a new privacy paradigm that manages the transition between modes of service and governance. Such an approach recognizes that technology offers interim solutions, not final resolution. Costs and acceptance risks are high; the preferred strategy is incremental and governance-directed. The task becomes one of management of the 'wickedness' of privacy problems, focusing on intersections of interests and competing imperatives.

Models for interaction show information exchange and tensions between what government wants to do, what technology allows, and the challenges to privacy. The citizen is at the intersection of information, service and governance. Each issue relates to the other; each influence proceeds in both directions. The citizen is the focal point of those with an interest in what she wants or supplies, but also exercises a legitimizing role for other functions. A focus on creating public value emphasizes ICT-enabled responsiveness to neutralize alienation from actors and processes while striving to neutralize alienation implicit in technologies replacing personal contact.

The quest for a model integrating privacy controls with public management and government is in its early stages.[64] If privacy is to be valued in recognizably traditional ways, it must be defined in such a way as lends it to control and redress. How this will change privacy is little understood and likely to be the subject of ongoing change. A viable model seems likely to require transformation as an inherent characteristic, to accommodate the changeable nature of ICTs and the range of responses to opportunities this offers. The model might accommodate the characteristics of legislation, or, more radically, it might propose an alternative paradigm susceptible to legal attention yet not be constrained by it. Business and government would have to overcome behaviour that deploys ICTs to disguise adapted systems, such as workplace surveillance that really only replaces older models of supervisor monitoring and intrusiveness. The legal system's deployment of privacy principles would have to recognize the implications of shifting capacity. Citizens would then decide on an appropriate balance between individual privacy as an absolute value, privacy as a broader social value, and gains from trading elements of these.

Conflicts between desires for privacy and desires for ever more innovative use of ICTs in public policy and management are too important to be delegated for resolution to specialist institutions and disciplines. Tools common to policy and management in addressing problems that do not always have neat, economical or elegant solutions can help define more sharply the questions we must ask and identify more clearly the paths we must take.

For this to succeed, public engagement must occur, to elicit and address citizens' concerns, and to canvass options that will engage the 'privacy pragmatists' and lead towards more constructive partnerships with policy and technology promoters. In this way the contradictory directions generated by pursuit of privacy can become agendas for continuing public deliberation rather than specialist debates leading to competing layers of flawed solutions.

## Notes

[1] *The Age* 23 and 25 September 2006 reports the story (http://www.theage.com.au/news/business/hp-chairwoman-ousted-over-snooping-scandal/2006/09/24/1159036415337.html; http://www.theage.com.au/news/technology/playing-keystone-kops-with-morality/2006/09/22/1158431899406.html).

[2] Horst W.J. Rittel & Melvin W. Webber (1973), 'Dilemmas in a general theory of planning', *Policy Sciences* 4, 155-169.

[3] Jane E. Fountain (2001), *Building the Virtual State. Information Technology and Institutional Change*, Washington D.C., Brookings Institution Press; C.J. Bennett & C.D. Raab (2003) *The Governance of Privacy: Policy instruments in global perspective*, Aldershot Hants., Ashgate, 3; P. Grabosky, R.G. Smith & G. Dempsey (2001), *Electronic Theft: Unlawful Acquisition in Cyberspace*, Melbourne, Cambridge University Press, 158.

[4] Andrew J. Charlesworth (2003), 'Privacy, Personal Information and Employment', 1 *Surveillance and Society*, 218.

[5] David Banisar & Sarah Andrews, 'The world of surveillance Pt 4: workplace privacy', http://www.austlii.edu.au/au/journals/PLPR/2000/54.html (29/09/06).

[6] Jim Nolan, 'Employee privacy in the electronic workplace Pt 1: surveillance, records and emails', http://www.austlii.edu.au/au/journals/PLPR/2000/51.html (29/09/06).

[7] Michael Ford (2002), 'Two Conceptions of Worker Privacy', 31 *Industrial Law Journal*, 142.

[8] See Nolan (2000), *loc.cit.* Presumably measuring the extent of such practices will invite remedial action.

[9] Kate Foord (2002), *Defining Privacy*, Victorian Law Reform Commission, Melbourne, 5.

[10] J. Braxton Craven, 'Personhood: The Right to be Let Alone', *Duke Law Journal* 1976, Issue 4, 705.

[11] Samuel D. Warren & Louis D. Brandeis (1890), 'The Right to Privacy', *Harvard Law Review* 4, 1890, 2.

[12] Ibid 6.

[13] David W. Leebron, 'The Right to Privacy's Place in the Intellectual History of Tort Law', 41 *Case Western Reserve Law Review*, 1990-1991, 779.

[14] Ruth Gavison, 'Privacy and the Limits of Law', 89 *The Yale Law Journal* 1980, 422-423.

[15] Julie C. Inness (1992), *Privacy, Intimacy, and Isolation*, Oxford University Press, New York.

[16] James Rachels, 'Why Privacy is Important', 4 *Philosophy and Public Affairs*, 1975, 326; Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object', 52 *Stanford Law Review*, 1999-2000, 1373.

[17] Daniel J. Solove, 'Conceptualizing Privacy', 90 *California Law Review*, 2002, 1127, 1143-1145.

[18] Raymond J. Wacks (2002), *Law, Morality and the Private Domain*, Hong Kong University Press, 241.

[19] *Australian Broadcasting Corporation v Lenah Games Meats Pty* [2001] HCA 63; 208 CLR 199; Kate Foord (2002), *op. cit*, 10.

[20] Kate Foord (2002), *op. cit*, 13.

[21] Ibid.

[22] Richard A. Posner, 'The Right of Privacy' 12 *Georgia Law Review* 1978, 393-404.

[23] Cohen, *loc. cit.*, 1395; Charlesworth, *loc. cit*,, 220.

[24] Rosa Ehrenreich, 'Privacy and Power', 89 *Georgetown Law Journal*, 2001, 2049-2061.

[25] Roger Clarke (1987), *Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme*, http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.htm; Graham Greenleaf (1987), *The Australia Card: towards a national surveillance system*, http://austlii.edu.au/itlaw/articles/GGozcard.htm; Jim Nolan, 'Privacy in the workplace – Part 1: legal issues', http://www.austlii.edu.au/au/journals/PLPR/1995/1.html

(29/09/2006).

[26] Examples: book control in libraries: http://www.theage.com.au/news/national/academics-may-get-look-at-banned-books/2006/10/03/1159641300001.html; http://www.theage.com.au/news/national/uni-terror-books-shelved-due-to-prosecution-fear/2006/10/02/1159641265066.html; research funding: http://www.theaustralian.news.com.au/story/0,20867,20415065-2702,00.html.

[27] For example, in France, Article 9 of the Civil Code, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the Labour Code.

[28] Peter P. Swire & Robert E. Litan (1998), *Avoiding a Showdown Over EU Privacy Laws*, The Brookings Institution, Policy Brief # 29, 2; Nolan (1995), *loc.cit.*

[29] See, for example, Catherine Delbar, Marinette Mormont & Marie Schots (2003), 'New Technology and Respect for Privacy at the Workplace', *European Industrial Relations Observatory on-line*, 8-10, http://www.eiro.eurofound.eu.int/2003/07/study/TN0303101S.htm; Directive 95/46/EC of the European Parliament and of the Council 1995 *On the protection of individuals with regard to the processing of personal data and on the free movement of such data*, http://europa.eu.int/comm/internal_market/privacy/law_en.htm. Other legislative instruments include: *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997, concerning the processing of personal data and the protection of privacy in the telecommunications sector; Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies, and on the free movement of such data; and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).*

[30] Even so, divergent outcomes have emerged in Europe: Michael Ford, *op.cit*., 142-143.

[31] Richard Fox (2001), "Someone to watch over us: Back to the panopticon?" *Criminal Justice* 1(3), 251-276, http://crj.sagepub.com/cgi/reprint/1/3/251 (29/09/06).

[32] Graham Sewell (1999), *On the Possibility of a Sociology of Workplace Surveillance*, Department of Management Working Paper in Human Resource Management, Employee Relations and Organisational Studies, University of Melbourne, 5.

[33] David Lyons (2001), *Terrorism and Surveillance: Security, Freedom, and Justice after September 11 2001*, Paper given at Privacy Lecture Series, http://privacy.openflows.org/pdf/lyon_paper.pdf; S. Zubboff (1988), *In the age of the smart machine: The future of work and power*, New York, Basic Books; Susan Bryant, 'Electronic Surveillance in the Workplace', *Canadian Journal of Communication* 1995, 20(4); M. Smithsimon, 'Private Lives, Public Spaces: The Surveillance State', *Dissent* 2003, 50(1), 43; Fox, *loc.cit.*

[34] F. Webster & K. Robins, 'I'll be Watching You: Comment on Sewell and Wilkinson', *Sociology* 1993, 27(2), 243.

[35] Banisar & Andrews, *loc.cit.*

[36] Kathleen M. Hallinan, 'Invasion of Privacy or Protection Against Sexual Harassment: Co-Employee Dating and Employer Liability', 26 *Columbia Journal of Law and Social Problems* 1993 Spring, 435.

[37] A. Fels (2003), 'The role of the privacy regulator in an era of transparency', 25th International Conference of Data Protection and Privacy Commissioners. Sydney, http://www.privacyconference2003.org (28 August 2004); Perri 6, Charles Raab & Christine Bellamy, 'Joined-up government and privacy in the United Kingdom', *Public Administration* 83 (1) 2005, 111-133.

[38] R.K. Chellappa, 'Contrasting expert assessment of privacy with perceived privacy: implications for public policy. http://www.digitalgovernment.org/library/library/pdf/chellappa.pdf (2 August 2004).

[39] MORI Social Research Institute (2003), *Privacy and Data-sharing: Survey of Public Awareness and Perceptions*, Research for the Department of Constitutional Affairs, London.

[40] MORI (2003), *op.cit.*; A.Westin (2001), 'Opinion surveys: what consumers have to say about information privacy', http://energycommerce.house.gov/107/hearings/05082001Hearing209/Westin309html (19 July 2003); S.J.

Stolfo, E. Johnson, T. Pavlicic & S. Jan (2003) 'Citizen's attitudes about privacy while accessing government and private websites: results of an online study', http://www.digitalgovernment.org/dgrc/dgo2003/cdrom/PAPERS/citsprivacy/stolfo.pdf (2 August 2004); Perri 6 et al., *loc cit*., 126.

[41] See Fox, *loc.cit*., 254-255. In Victoria, for example, there has been ongoing criticism of the use of speed cameras not for detecting offences, but for serving as proxy revenue raisers.

[42] Fox, *loc.cit.*

[43] M. Cooke, 'A space of one's own: autonomy, privacy, liberty', *Philosophy & Social Criticism* 1999, 25 (10), 23-53; Office of the Victorian Privacy Commissioner (2002). *Public Registers and Privacy*, Issue Paper 01.02, Melbourne, 1.

[44] Technology and Privacy Advisory Committee [TAPAC] (2004), *Safeguarding Privacy in the Fight Against Terrorism*, Washington DC, http://www.sainc.com/TAPAC (31 August 2004), ix.

[45] Fels, *loc.cit.*

[46] S.S. Dawes, V. Gregg & P. Agouris (2004), 'Investigations at the crossroads of social and information science', *Social Science Computer Review*, 22 (1), 5-10; J. Rimmer (2003), 'Australian Country Statement'. http://www.noie.gov.au (8 January 2004); National Office for the Information Economy (2003), *The Current State of Play: Online Participation and Activities 2003*, Canberra; HM Government (2002),. *In the Service of Democracy: a consultation paper on a policy for electronic democracy*, http://www.edemocracy.gov.uk/downloads/e-Democracy.pdf (6 January 2004).

[47] J. Seely Brown & P. Duguid (2000, 2002), *The Social Life of Information*, Boston MA, Harvard Business School Press.

[48] Stolfo et al., *loc.cit.*

[49] Westin, *loc cit.*; HM Government (2002), *Privacy and Data-Sharing: the Way Forward for Public Services*, Performance and Innovation Unit, Cabinet Office, London, Annex C.04-05; MORI, *op.cit.*, 7-9; D. Brown & M. Isakovic (2003), 'Security and privacy laws: striking the balance', Ottawa, Public Policy Forum, 10; Australian Government Information Management Office [AGIMO] and Institute of Public Administration Australia (ACT Division) (2004), *Future Challenges for E-Government*, Canberra, I, 146.

[50] For example: *The Age* 31 August ('Census should tell everything'), *Sydney Morning Herald* 11 August ('More questions than answers for the census'), 4 August ('Some census questions count more than others' – retention of information and release after 99 years), *The Financial Review* 8 August ('Take care in filling in e-census forms, experts warn').

[51] C.F. Kurtz & D.J. Snowden (2003), 'The new dynamics of strategy: sense-making in a complex and complicated world', *IBM Systems Journal* 42 (3), 462-483; S. Bell (2004), '"Appropriate" policy knowledge, and institutional and governance implications', *Australian Journal of Public Administration* 63 (1), 22-28.

[52] Nolan (1995), *loc.cit.*

[53] Other examples are: Australia's *Privacy Amendment (Private Sector) Act 2000* (Cth), s.7B, exempts in a wide basis employee records from privacy protection. The *Workplace Relations and Other Legislation Amendment Act* 1996 (Cth), s.89A(2), excludes privacy protection as an 'allowable' matter in industrial awards. And the Constitution contains no protection. See Fox, *loc.cit.*

[54] National Commission of Audit. 'Best practice in government activities', 5.2, http://www.finance.gov.au/pubs/ncoa/chap5.htm (27 November 2003); Office of the Victorian Privacy Commissioner, *op.cit.*, 7.

[55] National Audit Office (2002), *Better Public Services Through E-Government*; and *Government on the Web II*, London, The Stationery Office, http://www.GovernmentOnTheWeb.org/downloads/report_2000/9711vf_Government_on_the_web_II.pdf (27 November 2003).

[56] G. Grainger (1999), 'A co-regulatory scheme for Internet content: the Australian approach', http://www.aba.gov.au/about/public_relations/speeches.pdf (30 July 2004.); P. Coghlan (2000), 'The

principles of good regulation', in Productivity Commission and the Australian National University, *Achieving Better Regulation of Services*, Canberra, AusInfo, 31-57; Grabosky et al., *op.cit.*; Bennett & Raab, *op.cit.*; P. Grabosky & J. Braithwaite (1986), *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies*, Melbourne, Oxford University Press.

[57] HM Government, *Privacy and Data-Sharing*.

[58] K. Kernaghan (2003), *Integrated Service Delivery: Beyond the Barriers*, Prepared for the Chief Information Officer, Government of Canada, Brock University; Markle Foundation (2003), *Creating a Trusted Network for Homeland Security*, Second Report of the Markle Foundation Task Force, New York City NY, 6; AGIMO-IPAA, *op.cit.*

[59] Accenture (2002), *Technology in Government: riding the waves of change*, http://www.accenture.com (27 January 2004).

[60] Perri 6 et al., *loc.cit.*

[61] See Gordana Dodig-Crnkovic [2006], 'Privacy and Protection of Personal Integrity in the Working Place', Zentrum für interdisziplinäre Forschung / Centre for Interdisciplinary Research, Universität Bielefeld, http://www.idt.mdh.se/personal/gdc/work/Privacy_PersonalIntegrity_Workplace.pdf; Roger Clarke (1997), 'Privacy and Dataveillance, and Organsational Strategy', http://www.anu.edu.au/Roger.Clarke/DV/PStrat.html.

[62] See, for example, J.S. Fishkin (1996), 'The Citizen Engagement Round Table: deliberative polling', Institute on Governance, http://www.iog.ca/publication/cert1.pdf (28 August 2004); [1999], 'Deliberative polling as a model for ICANN Membership', Representation in Cyberspace Study, Berkman Centre for Internet & Society, Harvard Law School, http://cyber.law.harvard.edu/rcs/fish.html (28 August 2004); (2004), 'Deliberative polling: toward a better informed democracy', http://cdd.stanford.edu/polls/docs/summary/ (28 August 2004).

[63] Bennett & Raab, *op.cit.*

[64] For an early stage survey, see Vidya Moghe, 'Privacy management – a new era in the Australian business environment', *Information Management & Computer Security* 2003, 11/2, 60-66, http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=862840 (29/09/06); Clarke (1997), *loc.cit.*