Privacy, the war on terror and the modern Australian state

Title: Privacy, the war on terror and the modern Australian state
Author: I. Harriss and I. Coghlan
Author Address: iharriss@csu.edu.au; icoghlan@csu.edu.au
Conference Title: Conference Name: Hawaii International Conference on Arts and Humanities
Year of Conference: 2007
Conference Location: Honolulu, Hawaii USA
Editor: Publisher: Hawaii International Conference on Arts and Humanities
Pages: pp. 2154-2167
URL: http://www.hichumanities.org
Keywords: Privacy, Terror
Abstract: Privacy is a concept that is philosophically vague and legally weak in the Australian common law. Considered in philosophical terms, the issue has been bedevilled by spatial, bodily and proprietary concepts. Meanwhile, threats to privacy and data security multiply as technological change creates more privacy-invasive opportunities. This is particularly so in the post-September 11 world, where the surveillance powers of the State are in the ascendant. At the moment there are two parallel streams: a non-State regime in which protection of individual privacy is fragmented and weak; and a State-driven one based on profiling and interventionist strategies of risk identification and management. Encryption enhances privacy, but in the contemporary climate it conflicts with the interests of the State. The ethical issues need to be clarified before they can be resolved.
CSU ID: CSU289241
PRIVACY, THE WAR ON TERROR AND THE MODERN AUSTRALIAN STATE

Ian Harriss and Ian Coghlan
Charles Sturt University, Albury NSW 2640 Australia
iharriss@csu.edu.au, icoghlan@csu.edu.au

ABSTRACT

Privacy is a concept that is philosophically vague and legally weak in the Australian common law. Considered in philosophical terms, the issue has been bedevilled by spatial, bodily and proprietary concepts. Meanwhile, threats to privacy and data security multiply as technological change creates more privacy-invasive opportunities. This is particularly so in the post-September 11 world, where the surveillance powers of the State are in the ascendant. At the moment there are two parallel streams: a non-State regime in which protection of individual privacy is fragmented and weak; and a State-driven one based on profiling and interventionist strategies of risk identification and management.

Encryption enhances privacy, but in the contemporary climate it conflicts with the interests of the State. The ethical issues need to be clarified before they can be resolved.
Privacy, the War on Terror and the Modern Australian State: From the Embodied Self to the Digital Persona in a post-September 11 World

The aim of this paper is not to provide a detailed account or analysis of Australian legislative responses to terrorist threats in the post-September 11 world. Our aim is both narrower and broader than that. The aim of this paper is to explore cultural, political and legal aspects of privacy in an Australian context, while recognising that intersecting discourses and values are now rendered more complex and problematic by the parallel emergence of terrorist threats.

In this paper we argue that the Australian law relating to privacy is in a state of confusion and contradiction in the post-September 11 world. There are now two divergent streams, each with its own paradigm, and each with its own history and trajectory. First, there is a weak statutory regime developed from a fragmented common law tradition; and there is a second stream, legitimised in the age of terror, that seeks to use the technology of a surveillance society in order to enhance collective security.

The first stream, which is based on nineteenth century conceptions of the liberal autonomous individual, fails in fundamental ways to protect individuals. The legislative regime is a complaints-based framework based on vague concepts of fair dealing, and it contains so many exemptions that its supposed purpose is effectively negated. Moreover, the legislation is contained in numerous Acts at both State and Commonwealth level.

---

1 See, for example: Privacy Act (Cth) 1988; Privacy Amendment (Private Sector) Act (Cth) 2000; Information Privacy Act (Vic) 2000; Workplace Video Surveillance Act 1998 (NSW); Surveillance Devices Act 1999 (Vic). It is not the purpose of this paper to undertake a detailed analysis of the legislation, but rather to discuss the conceptual issues, particularly of an ethical nature, that arise from the overall approach adopted in the legislation.
Such a mish-mash has emerged from a common law in which there is no right to privacy as such. At common law, threats to the integrity of the individual are conceived in terms of boundaries that protect the bodily integrity, and the public character, of the individual from external invasions. Philosophically, this conception of privacy is based on the protection of a physically embodied person. In the Australian philosophical imagination, the liberal autonomous individual stands tall and alone. Historically, the rights of the individual have therefore been reduced to a set of boundaries that must not be transgressed.

Considered in terms of both legal and cultural discursive strategies, the issue of privacy has therefore been dispersed into legal categories such as trespass, assault, nuisance, defamation, passing off, infringement of intellectual property rights, and breach of a duty of confidentiality. As causes of action, these were generally adequate for most nineteenth and twentieth century violations of an individual’s privacy. The law was concerned to prevent discrete or singular transgressions across the various boundaries that separated the individual from the public world. The aim was the creation of a civil society based on non-violent social interaction.

The imaginative power of this conception can be traced back to Thomas Hobbes. In the Hobbesian world view, other human beings are potential threats. In effect, the law — or the sovereign entity in whom power is contractually vested — exists in order to prevent transgressions against the individual. Such bodily and proprietary based conceptions are effectively irrelevant to the digital world, where the threat to the individual arises not from a singular transgression of any discernible boundary but from the anonymous, continuous accumulation of data relating to the individual’s digital persona. Moreover, the threat is intensified by the potential to merge data bases.

**September 11 and the Rise of the Surveillance State**

The second paradigm, based on monitoring and surveillance by the State, aims to enhance collective security by applying computer technology to the tasks of risk identification and assessment. This represents a departure from traditional criminal law because there is a focus initially on the task of identifying individuals of interest, supported by subsequent endeavours to collect information relating to their connections, associations and patterns of communication. Operations within this surveillance paradigm may even focus on ideas that an individual holds, or is presumed to hold. In all such cases there need be no existing evidence of a crime, or even of an intention to commit a crime. Such an approach represents a shift away from a criminal law paradigm to one of risk identification and management. Such an approach is inherently pre-emptive, and it is inevitably based on profiling (Lyon, 2002, 2003). Considered from this perspective, the paradigm is potentially in conflict with the values of a free and tolerant multicultural society.
Two Paradigms: A New Confusion added to Old Confusions

The ethical confusions that arise from the existence of these two paradigms reflect not only the tensions, contradictions and confusions of contemporary Australian culture in the context of multiculturalism, globalization and a post-September 11 environment; they also reflect the ambivalent potential of the digital revolution. Digital technology poses an enormous threat to individual privacy, yet it also enhances collective security in the war against terror.

Individual freedom and collective security, however, are not necessarily antithetical; and nor are democratic rights inconsistent with the existence of a strong State. The question that needs to be asked is this: how can safeguards for ordinary citizens be strengthened, and yet how can the State also have the powers it needs in order to prevent terrorists from achieving their objectives? Before this question can be addressed, other questions need to be answered: who determines if a citizen is or is not an ordinary citizen, and when, and by what processes, and by which persons or bodies, is such a determination to be made?

It is crucial that the two paradigms be kept distinct, and it is crucial that processes be put in place in order to ensure that this is the case. If we are effectively looking at the emergence of parallel systems of law and ethics, then the question is whether Western democracy is sufficiently sophisticated and flexible to accommodate two parallel regimes. There is, of course, one other difficult question: how do we keep those regimes separate on an ongoing basis?

Australian Common Law Treatment of Privacy and Individualism: Protection of the Body and Property

Unlike the USA, which has both a Bill of Rights and a tort of privacy, Australian conceptions of privacy have to be teased out of a dispersed set of laws and philosophical principles. These, in turn, can only be understood in relation to Australian culture. The Australian character is robustly individualistic, and it is marked by a healthy resistance to authority. These features are rooted in the convict origins of Australian society, and also in the myth of egalitarianism (Carter, 2006). In the early twentieth century, in the decades following Federation, Australian democracy was well ahead of Europe in its headlong surge to modernity. On the other hand, there is also a recognition that the State has a role to play in civil society.
These elements came together and found expression in one of the early landmark cases relating to privacy: *Victoria Racing Park and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479. In this case conceptions of property, and a desire to prevent the transgression of boundaries, prevailed. The matter in dispute involved a radio station that had sought to avoid payment of rights to broadcast by setting itself up outside the ground, but with a clear view of the races that were taking place inside the ground. Importantly, no trespass had taken place.

As generally understood, this case was taken to stand for the principle that there was no general right to privacy at common law. It was, of course, a poor set of facts from which to draw such a conclusion. The relationship between the parties was a relationship between impersonal organisations rather than between individuals, and the issue at stake was essentially a commercial one rather than an intimate or emotional aspect of an individual's existence. Rather than privacy, the case turned on the issue of who had proprietary rights to the open spaces of the racecourse and the very public spectacle that took place there. There was little about these facts that was private other than in the proprietary sense of the term.

The more recent Queensland case of *Grosse v Purvis* [2003] QDC 151, however, suggests that the issue is no longer as settled as it recently seemed.

**Privacy, Data and the Digital Persona**

A conception of privacy based on spatial, bodily, and proprietary metaphors, and on singular or discrete physical acts, is ill-suited to the present-day threats posed by data collection, merged databases, cookies, web-bugs, cyber tracking and dataveillance. These acts do not involve a trespass as conventionally conceived, and nor do they constitute an assault, or even a nuisance, as the law currently stands. Whereas conventional conceptions of invasions of privacy evoke a spatial metaphor, or a sense of inner and outer, in a digital environment we are faced with a situation in which there has been a scattering of personal data in a decentred cyber world beyond our sensual experience. Individuals and organisations unknown to us aim to collect and amalgamate otherwise innocuous pieces of data of a more or less public nature, for the purpose of constructing a digital persona. On its own, little of this data would be considered private, at least in the traditional sense of the term. Today, the threat to individual 'privacy' often arises not from any particular act, or from any particular piece of data *per se*, but from the pervasive, constant, cumulative and secretive nature of the process. It is the loss of autonomy that is the threat, and not the invasion of our private or emotional life.
A number of interrelated trends have exacerbated this threat: rapid developments in telecommunications, informatics, biotechnology and genetics have coincided with a convergence of new technologies. The result has been an explosion of sensitive, centralised and cheaply retrieved data that is now stored, not in paper format at separate geographic locations, as was once the case, but in cheaply and easily accessible data bases that can be merged with the click of a mouse (Waters, 1997). As Kirby (1998: 5) observes, the technology of the internet ‘tends to favour the spread of information’ while ‘the protection of competing values is weak’.

This is the calculus of a surveillance society in which traditional liberties based on ex-poste evidence are in retreat and the new surveillance technology and will of the State, based on ex-ante assessments, are in the ascendancy (Lyon, 2001; Lyon, 2002).

Perhaps this explains the observations of those such as Robert Warren (2002: 614), who notes the conflation of the public and private and the subjugation of civil society to an increasing militarisation of urban space. Clearly, in the aftermath of September 11 the modern State will seek to use all available technology at its disposal to analyse and evaluate a vast amount of personal data. (Etzioni, 2002: 274-80; Hunter, 2002). Technologies, political will and administrative capabilities have coalesced at a juncture where it is possible to track cars and mobile phones, and to integrate this data with increasingly sophisticated genetic and biometric data, as well as with data bases developed by various private organisations at different cyber locations.

The problem here is that when any person or organisation is given power, that power must be codified and constrained. The argument that the State should have certain rights might be sound in principle but it is a right that is subject to abuse. Indeed, as Simon Davies (2001) cautions, such arguments feed ‘on hypocrisy, deception and a total absence of any intellectual or analytical foundation, resulting in unreasonable extensions of surveillance’. For this reason there is a strong argument that the degree of independent external scrutiny should rise in proportion to the concessions that are made in the interests of public safety. This approach would place the burden on government to demonstrate that such concessions are needed. For this purpose, the bar would be set very high (Strossen, 2001).

**The Issue of Privacy-Enhancing Technologies: Privacy, Encryption and the State**

Some American observers see cryptographers as existential heroes in a new techno-frontier, defeating the malevolent and conspiratorial impulses of national government. Westin (1998), for example, in his keynote address to a 1998 conference on Privacy and the Internet, invoked
Western frontier imagery when he said: 'As in the earliest days in America, the Internet abounds with modern day cattlemen, sheep-herders, farmers, saloon keepers, whores, and hacker-gunmen, with the influences of the schoolmarm, minister, sheriff, and judge also struggling to be heard and felt'. Mike Godwin (2003:158) suggests that 'at a deep level, the philosophical issues raised by cryptography...centre on the question of whether we believe that human beings, once empowered to speak anonymously and secretly, are more likely to use their new powers unjustly, to do harm to others, than to act with integrity'.

In the post-September 11 world (Graham, 2002; Lyon, 2003), can such a utopian ontology of the human subject really be the basis for legal and ethical thinking about the issue of data security in a global environment of transnational terrorist cells?

Godwin can only conduct his argument along these lines by fixating on one principle and ignoring all other competing principles, such as risk identification and management. The management of risk, however, is not antithetical to the defence of civil liberties, and nor is a strong State antithetical to the preservation of either individual freedoms or individual autonomy. Only a strong State is capable of preserving the processes and procedures, the checks and balances, and the dispersal of decentred governmental and corporate power that are essential for the preservation of privacy and individual rights.

Does the State have a reasonable and legitimate interest in searching an individual's private location in cyberspace, just as it has an interest in searching inside real private spaces, such as houses and workplaces? Such a right in the physical world is commonly accepted, so long as it is subject to proper legal process. The issue at hand here is whether the processes and protocols of real space apply, or can be reasoned by analogy to apply, in the digital world.

Cryptography should not be seen in essentialist terms, as though it naturally and automatically enhances the value of privacy. There is always a human context to the use of technology. In certain circumstances encryption can be used to perpetrate the most serious violations of individual privacy. The Privacy and Innovation Unit Report on encryption provided to the UK Government in 1999 highlights some key examples of such violations in the area of child pornography, where encrypted images were sent to contacts around the world (1999: 7).

The problem with powerful encryption, as Amitai Etzioni (2002: 265) observes, is that 'it is qualitatively different from the impact of other privacy-enhancing technologies'. He argues that in the past the main factor that constrained public authorities when new technologies emerged was the obsolescence of existing laws. In the case of strong encryption, however, 'the technology imposes its own barrier'. The problem can no longer be solved by updating
the law. Public authorities now understand that 'no court order can enable strong encryption to be broken'.

Cryptography undoubtedly makes an important contribution to internet security, and there is a strong case for its universal availability, but there is also a strong argument that it should be subject to the checks, controls and due processes of civil society. Etzioni (2002: 281-82) is surely right when he says that 'it is difficult to sustain the argument that the government should be unable to decrypt any messages or be unable to gain the authority to do so'. The most important objectives are to determine which messages can be decrypted; under what circumstances and by what processes permission to do is to be granted; who is to verify that independently determined limits have been observed; and by what means such verification will be undertaken.

The need to address these issues is urgent. Denning (1996) suggests that 'the widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wiretaps) and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight'. She argues that the consequences would be 'devastating'. In her view, computers and telecommunications systems would 'become safe havens for criminal activity' of various kinds: tax evasion, money laundering, industrial espionage, the purchase and sale of electronic information on black networks, the corruption of corporate records, and the rendering of corporate and other information inaccessible. Denning (1996) suggests that 'by strengthening the integrity of evidence and binding it to its source, cryptographic tools for authentication are a forensic aid to criminal investigations'.

In a democracy, the desirable principle is that power should be divided and then dispersed in such a way that it is subject to discussion, review and even contestation. Negotiation and due legal processes ideally exist wherever power is present.

One option is to develop legislation designed to encourage the wide use of trusted third parties. This would have the effect of maintaining data security, privacy and confidentiality under normal circumstances while providing for a dispersal and fragmentation of power. There is also one other benefit: as Greenleaf (1996) suggests, third parties are easier to serve with warrants while maintaining covert operations. If Trusted Third Parties are licensed, then law enforcement agencies are able to pursue serious crime by establishing procedures by which encryption keys would be disclosed to them. These procedures would have safeguards similar to those that already exist with respect to telecommunications legislation.
CONCLUSION

The Australian legislation is notable not for its strict protection of privacy, but for the large number of exemptions it allows. In this context, Davies (2001:7) is surely correct when he argues that ‘(t)he preservation of privacy should not be viewed as an encumbrance that can be diluted through ‘public interest’ exemptions, but as a public interest in itself’. 
REFERENCES

Cases

Grosse v Purvis [2003] QDC 151

Victoria Racing Park and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479.

Statutes

Privacy Act (Cth) 1988
Privacy Amendment (Private Sector) Act (Cth) 2000
Information Privacy Act (Vic) 2000
Workplace Video Surveillance Act 1998 (NSW)
Surveillance Devices Act 1999 (Vic)

Other References


