CHAPTER SIXTEEN

PRIVACY REGULATION AND e-RESEARCH

Andrew Hayne[1]

INTRODUCTION

The Office of the Privacy Commissioner appreciates the kind invitation from the Law Faculty at Queensland University of Technology to present at the 2007 Legal Framework for e-Research Conference. This legal framework project coincides with a key period for privacy regulation in Australia, most significantly due to the current inquiry into privacy law being conducted by the Australian Law Reform Commission (ALRC). At the same time, public policy is increasingly examining how best to facilitate research interests through the use of personal information. The Office notes, for example, the National Data Network initiative,[2] as well as the inquiry conducted by the Productivity Commission[3] into the role of research in Australia, to which the Office made a submission.[4]

In this chapter I aim to provide a brief overview of federal information privacy regulation, particularly as it applies to health and medical research, as well as to thumbnail possible opportunities for reform that may emerge from the current ALRC inquiry. These opportunities are

---

[1] Deputy Director of Policy, Office of the Privacy Commissioner.

[2] <http://www.nationaldatanetwork.org/ndn/ndnhome.nsf/Home/Home>.

[3] See Public Support for Science and Innovation <http://www.pc.gov.au/study/science/finalreport/index.html>.

[4] The Office of the Privacy Commissioner, *Submission to the Productivity Commission: Research Study into Public Support for Science and Innovation* (2006) <http://www.privacy.gov.au/publications/sub_prod_science072006.html>.

discussed in detail in the Office's submission to that inquiry, available from our website.[5]

OVERVIEW OF THE *PRIVACY ACT* 1988

An important starting point in understanding privacy regulation is to recognise that the *Privacy Act 1988* provides principle-based, technology neutral regulation.

The intention of principle-based law is to emphasise the objectives of the law rather than prescribe what the regulated party may do.

Principle-based law is aimed at encouraging organisations to understand the policy underpinning behind the law and adapt their practices accordingly; not just to prevent intervention from the regulator, but because they recognise the purpose and intent of the law.[6]

Principle-based law also sits comfortably with government policy favouring co-regulation, whereby business is left to pursue solutions that are appropriate to their industry, structure and circumstances, while still meeting the policy objectives of the regulation.

Technological neutrality is intended to recognise the inherent difficulty of keeping statute law up to date with new and emerging technologies.

The Office believes that the *Privacy Act* should continue to be technologically neutral. It is often difficult to envisage how technology will evolve or what new technologies may emerge. It would therefore be extremely difficult to respond effectively to dynamic technological development.[7]

At the same time, to accommodate particular emerging technologies that may create privacy risks, the Office has proposed to the ALRC inquiry that the *Privacy Act* should provide the flexibility for the Privacy

---

[5] The Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/alrc280207.html>.

[6] See also Karen Curtis (Privacy Commissioner) 'Reducing overlap, duplication and inconsistency' (Speech delivered at the Australian Regulatory Reform Evolution 2006, Canberra, 24 October 2006) <http://www.privacy.gov.au/news/speeches/sp05_06.pdf>.

[7] This is discussed in further detail in the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) Chapter 11 <http://www.privacy.gov.au/publications/submissions/alrc/c11.html#L25052>.

Commissioner, subject to Parliamentary oversight, to make binding codes that go to specific acts or practices that may be enabled by new or emerging technologies.[8]

MEANING OF 'PERSONAL INFORMATION'

It is important to recognise that the *Privacy Act* focuses its regulatory functions on information privacy. In turn, the scope of information privacy is determined by the meaning of 'personal information'.

The statutory definition of personal information is contextual, in that it refers to information or opinion about an individual whose identity is apparent *or can be reasonably ascertained*. Clearly, whether an identity can be reasonably ascertained will be determined by the context in which that information is held, including the availability of technologies that may reasonably *re-identify* information that is putatively *de-identified*.

For example, Robert Gelman, in *Public Record Usage in the United States*,[9] cites research that reveals:

> … the Cambridge, Massachusetts voter registration list has 55,000 voters. Twelve percent of voters have unique birthdates. So if a person of voting age lives in Cambridge, the voter might be identified just from the birthdate on the voter list. With birthdate and gender, 20% of voters are unique. With birthdate and five-digit zip code, 69% are unique. With birthdate and nine-digit zip code, 97% are unique. More broadly, 87% of Americans can be identified just by birthdate, five digit zip code, and gender.

More recently, the Office notes the widely publicised case whereby 20 million putatively de-identified internet search records on 650 000 AOL users were made publicly available. By examining linkages between different searches, a *New York Times* journalist found that:

---

[8] This is discussed in the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) Chapter 6 and Chapter 11 <http://www.privacy.gov.au/publications/alrc280207.html>.

[9] Available at <http://www.cnil.fr/conference2001/eng/contribution/gellman_contrib.html>.

> It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga.[10]

In the view of the Office, this contextual element is one of the strengths of the definition, allowing it to respond to change and technological advance, as well as the particulars of a given context. In order to alleviate any confusion generated by the flexibility of the term, the Office intends to issue further guidance material on the meaning of 'personal information' in a regulatory context.[11]

STATUS OF 'HEALTH INFORMATION' IN PRIVACY REGULATION

The *Privacy Act* also deals expressly with health information, which is defined in broad terms and exists as a subset of personal information.[12]

Consistent with the second reading speech for the Privacy Amendment (Private Sector) Bill 2000, the community expects that such health information will be afforded privacy protections that are in addition to those applying to non-health information.

In the second reading speech for that Bill, the then Attorney-General, the Hon Daryl Williams QC, said that:

> The government recognises that the Australian public considers their health records to be particularly sensitive … The bill provides additional protections in relation to the use and disclosure of health information, as such information is

[10] M Barbaro and T Zeller 'A Face Is Exposed for AOL Searcher No. 4417749', *New York Times*, 9 August 2006, <http://www.nytimes.com/2006/08/09/technology/09aol.html?ei=5087&en=fc3fb3310bf58bd7&ex=1171771200&excamp=mkt_at1&pagewanted=all>.

[11] The adequacy of the definition of 'personal information' is discussed in the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) Chapter 3 <http://www.privacy.gov.au/publications/submissions/alrc/c3.html#Personal>.

[12] 'Health information' is discussed further in the Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001) A.3.2 <http://www.privacy.gov.au/publications/hg_01.html#a32>.

> clearly considered by the community to be particularly sensitive.[13]

REGULATION AFFORDED BY THE *PRIVACY ACT*

In regard to the *Privacy Act's* jurisdiction, the *Act* sets out 11 principles, called the Information Privacy Principles, which apply to most Australian Government agencies, and 10 principles, termed the National Privacy Principles, which apply to all private sector bodies with turnover greater than $3 million, as well as to all health service providers in the private sector.

Significantly, neither set of privacy principles apply to state agencies, including public health systems, nor to most public universities, except where established under Commonwealth law.

The two sets of principles, while having differences in a number of areas, share underlying objectives, including ensuring that individuals know who has personal information about them, what will be done with it and that it will be handled with appropriate security.

Common to both principles is the general requirement that personal information, including health information, should only be used or disclosed for the purpose for which it was initially collected, unless an exception specified in the *Privacy Act* applies - I will return briefly to these exceptions and secondary purposes shortly.

However, notwithstanding the commonalities between the principles, the Office is of the view that maintaining two sets of privacy principles causes unnecessary complexity for all stakeholders. Law reform could, and should, usefully include amendment to create a single set of privacy principles.[14]

---

[13] The Hon Daryl Williams QC, Second Reading Speech Privacy Amendment (Private Sector) Bill 2000 <http://parlinfoweb.aph.gov.au/piweb/TranslateWIPILink.aspx?Folder=HANSARDR&Criteria=DOC_DATE:2000-11-08%3BSEQ_NUM:8%3B>.

[14] The proposal for a single set of privacy principles is discussed throughout the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007), though most directly in Chapter 4 <http://www.privacy.gov.au/publications/submissions/alrc/c4.html>.

OFFICE VIEW ON MEDICAL RESEARCH

The Office recognises that there is an important social interest in enabling medical researchers to have access to health information in certain circumstances. The *Privacy Act* is not intended to restrict important medical research. While health information, being sensitive information, is afforded extra protection under NPPs, the *Privacy Act* recognises the desirability of health and medical research by enabling health information to be collected, used and disclosed for these purposes, in some cases, without consent.

FUNCTIONS OF THE PRIVACY COMMISSIONER

It is useful to note that the Privacy Commissioner has express functions under the *Privacy Act* concerning health and medical research. Most significantly, these functions include to approve Guidelines made by the National Health and Medical Research Council (NHMRC) under sections 95 and 95A of the *Privacy Act*.[15] These guidelines provide a framework for non-consensual research, and I will return to them shortly.

The Privacy Commissioner also receives reports from the NHMRC on the operation of these Guidelines. These reports serve important oversight functions for the operation of the guidelines. To promote transparency, the Office can see merit in progressing to a point where these reports are made publicly available.

QUESTIONS FOR THE RESEARCHER

For the researcher, the application of the *Privacy Act* first turns on whether the data involved meets the definition of personal information. If it does not, then neither set of privacy principles apply.

This again raises the issue of what does personal information mean – whether or not data satisfies the statutory definition will depend on the circumstances in which it is held and, crucially, whether an individual's identity is apparent or reasonably ascertainable.

---

[15] The section 95 and 95A Guidelines are available at <http://www.privacy.gov.au/health/guidelines/index.html#2>.

If it is established that research data is regulated as personal information, the *Privacy Act* offers a number of mechanisms by which it may be handled for research purposes. These include where the information was initially collected for the primary purpose of conducting that research project.

The Office of the Privacy Commissioner also recognises that the use of personal information for the *secondary* purpose of research is of significance to researchers. It is perhaps most common for health information, in particular, to be collected for purposes other than research, such as the clinical care of the individual. Nonetheless, this information may be of considerable value in a research context.

Further, as shared electronic health records systems evolve, there would seem every chance that richer repositories of health information may emerge.[16]

The *Privacy Act* provides various mechanisms by which health information may be used for the secondary purpose of research.

For example, this may occur with the consent of the individual; in this regard, researchers may usefully bear in mind that consent may be express or implied, and may be written or verbal.

The Parliament, in recognition of the important role of health and medical research, has also acknowledged that, in some circumstances, health information should be available for important research activities where it is impracticable to gain the individual's consent.

The Office has issued guidance material explaining that impracticability may include where:[17]

---

[16] The issue of electronic health records is discussed at question 8–5 of the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L20635>. The Office has also discussed its views on EHRs more generally in submissions to the former HealthConnect project office, see Office of the Privacy Commissioner, *Submission on the HealthConnect Business Architecture* (2005 Version 1.9) <http://www.privacy.gov.au/publications/hlthcnnctsub.pdf>.

[17] The question of when consent may be impracticable is discussed at question 8–30 of the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L22503>.

- individuals may be uncontactable due to there only being old records available;
- the individuals of interest may be part of a demographic group that is typically difficult to contact, including remote, transient or indigenous groups;
- the sheer number of records involved may cause excessive logistical problems; and
- where seeking consent may in itself fundamentally and unavoidably undermine the integrity of the research methodology.

This mechanism for non-consensual research is facilitated through sections 95 and 95A of the *Privacy Act*.[18] These sections apply, respectively, to Commonwealth agencies and to private sector organisations.

These sections require the NHMRC to make guidelines, approved by the Privacy Commissioner, setting out under what circumstances non-consensual research may proceed.

The guidelines provide a framework to ensure privacy protection of health information that is collected or used or disclosed in the conduct of research. Under the guidelines, Human Research Ethics Committees (HRECs) are required to the approve research, including by considering the affect on the privacy of the research subject.

THE NEED TO HARMONISE SECTIONS 95 & 95 OF THE *PRIVACY ACT*

While the Office broadly supports this form of mechanism, it is apparent that, while having similar policy objectives, sections 95 and 95A display a number of inconsistencies. Agencies, for example, may handle any form of personal information for the purpose of medical research, while organisations are limited to handling 'health information' albeit for apparently much broader purposes of 'research relevant to public health or public safety'. This would appear to limit, for example,

[18] Sections 95 and 95A are available at <http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/previewlodgmentattachments/409069FCABD20271CA25725C008385B5/$file/Privacy1988_WD02HYP.htm#param220>.

the linking of health information with non-health information, notwithstanding that such linkages may be for public health or safety research.

Stakeholders have previously expressed the view that the existence of two sets of Guidelines regulating the public and private sectors was causing difficulties for researchers and ethics approval processes.[19]

The differing requirements of Sections 95 and 95A are inconsistent and confusing. Accordingly, in our recent submission to the ALRC inquiry, the Office has pointed to the potential benefits of a simplified framework for the regulation of how personal information may be handled, without consent, for health related research by organisations and agencies.

REVIEWING THE *PRIVACY ACT*

As I have mentioned already, the reform of privacy law is very much a live matter, and may have significant implications for research.

Since 2003, there have been three reviews instigated of the current state of federal privacy regulation in Australia, albeit with different objectives and terms of reference.

The reviews conducted by the Office of the Privacy Commissioner and the Senate Legal and Constitutional Affairs Committee have led up to the current inquiry by the ALRC.

WHAT MIGHT REFORM OFFER MEDICAL RESEARCH?

An important question is to ask, what might useful law reform look like, particularly as it affects health and medical research?

Retain Strong Protections for Health Information

The Office of the Privacy Commissioner would expect that any such reform should proceed from the recognition of the importance individuals place on how their health information is handled.

[19] This, and other research related issues, was discussed in the Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005) <http://www.privacy.gov.au/act/review/review2005.htm#7_3>.

Individuals' engagement with the health sector remains largely premised on the assumption that they can rely on providers to maintain the privacy and confidentiality of their health information. Drawing on the World Medical Association's recent 2006 Declaration of Geneva, providers assert that they will 'respect the secrets that are confided in me, even after the patient has died'.

The Office believes that codified privacy regulation, which seeks to balance the public interest in privacy, with the public interest in health and medical research, plays an important role in sustaining community confidence about how health information may be used for research purposes.[20]

From this basis, the Office supports the ongoing role of HRECs as providing appropriate institutional oversight of human research.[21]

While submissions to the Office's 2003 review referred to concerns about the adequacy of HREC resources, and whether HREC decision making may, on occasion, be unnecessarily conservative in regard to privacy, the Office remains of the view that the existence of institutional ethical oversight has served Australia effectively and promoted community confidence that abuses committed in the name of research in other countries, are unlikely to happen here.

Harmonise the Section 95 and 95A Mechanisms

At the same time, the Office has proposed that simplifying and harmonising the section 95 and 95A processes, including by making a single, common set of guidelines for Commonwealth agencies and the private sector, would assist HREC decision making by reducing unnecessary complexity.[22] The Office has already committed to work

[20] This theme is also discussed in the Office of the Privacy Commissioner, *Research Study into Public Support for Science and Innovation: Submission to the Productivity Commission* (2006) <http://www.privacy.gov.au/publications/sub_prod_science072006.html>.

[21] The role of HRECs in providing institutional oversight of research is discussed at question 8–31 of the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L22607>.

[22] The question of harmonising the section 95 and 95A mechanisms is discussed in detail at question 8–32 of the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L22695>.

with the NHMRC to explore ways to simplify reporting obligations faced by HRECs.

One Set of Privacy Principles

More generally, the proposal for a single set of privacy principles, common to agencies and organisations, would similarly lessen regulatory confusion as to how research may be undertaken.

Clarify Interaction with State and Territory Law

The Office has also proposed reform to the *Privacy Act* to remove any uncertainty as to the role of State and Territory privacy laws to the private health sector.[23]

In this regard, the Office has previously stated that the best advice available to it is that where an act or practice is regulated by the Commonwealth *Privacy Act*, then it is not regulated by a State or Territory privacy Act. On this basis, the State and Territory health privacy Acts are restricted in their application to the relevant State or Territory public sector.

Equally though, the Office has recognised that the matter is not fully settled and that other parties may have differing advice. The Office's view is that this lack of certainty creates a major potential obstacle to effective and consistent privacy regulation in the Australian federal system.

The Office has proposed that amending the *Privacy Act* to make clear that its provisions 'cover the field' for the regulation of private sector health service providers would be a significant step toward reducing possible uncertainty for those bodies, including in research contexts.

Issues for e-Research

An issue that may have particular import for the e-research agenda include ensuring clarity and certainty around the meaning of 'personal information', particularly in light of the contextual element introduced in its definition through reference to someone's identity being 'reasonably

[23] See question 8–2 of the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L20540>.

ascertainable'. The Office has committed to providing further guidance on this issue.[24]

Perhaps also significant are the provisions regulating transborder dataflows of personal information. Advances in information technology have allowed information to be sent across the world with speed and efficiency. With the advent of inexpensive high-speed internet connections and the growth of the global economy, Australian agencies and organisations are increasingly operating across national borders. This will equally apply to researchers.

Currently, personal information may only be sent overseas subject to the requirements of National Privacy Principle 9, which include that such transfers should occur where comparable privacy protections apply, either in law or by other agreement, or where the individual consents.

Further analysis may be required to flesh out the privacy law obligations involved in exchanging personal information across borders for research, particularly in regard to such matters as ensuring legal compliance and the role of HRECs in an international context.

The question of how best to regulate datasets established for broad research purposes, such as health registers, remains an important one.[25]

The Office has noted that many such registers have benefited from the certainty of being established under state or territory law, or on the basis of individual consent.

The Office notes that, with the expansion of electronic health records, it may become increasingly difficult to quarantine research registers from other health information systems. The move towards electronic health records may put increasing pressure on health records to be multi-functional, where they are used for patient-care, as well as epidemiological and other research objectives.

The role of consent in the context of multi-purpose data registers seems unclear, particularly where it may not be known what specific research

---

[24] The meaning of 'personal information' was discussed in the Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005) <http://www.privacy.gov.au/act/review/review2005.htm#8>.

[25] Health registers and datalinkage are discussed at question 8–33 of the Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31* (2007) <http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L22811>.

will be undertaken in the future and, therefore, individuals may not be adequately informed so as to offer truly meaningful and valid consent.

The Office sees merit, therefore, in specific legislative provision being made for the establishment of health data registers that are intended to serve broad research objectives. Doing so would recognise both the value of such registers, and the sensitivity of the information they contain and would offer the certainty, parliamentary oversight and scrutiny needed to sustain community confidence.

CONCLUSION: GOOD PRIVACY SUPPORTS GOOD RESEARCH

In closing, the Office is well aware of criticisms from some stakeholders that privacy regulation unreasonably impedes research in some contexts. The Office believes that regulatory reform to promote simplicity and overcome regulatory uncertainty would likely address many of these concerns.

More generally, though, far from being an obstructing factor, in the Office's view, privacy regulation is a necessary and supporting condition for serving the public interest in the benefits of research. The relationship of trust between health service providers and individuals is vital for sustaining public confidence in the health sector, their participation in effective treatment and the resulting quality of medical research.