UNSW Cyberspace Law and Policy Centre Symposium: Meeting Privacy Challenges – The ALRC and NSWLRC Privacy Reviews

Thursday 2 October 2008

Panel Session 6:

How well do the ALRC/NSWLRC proposals contribute to limiting the growth of a Surveillance Society?

Pauline Wright, Vice President, NSW Council for Civil Liberties

---

Overview

It's useful to remember that not everyone shares the view that privacy ought to be protected. When the issue of surveillance is raised in the context of privacy, I'm often asked, as a civil libertarian, "if you have nothing to hide, what have you got to worry about?"

That argument is, at worst, disingenuous and, at best, naive.

It assumes a fair and balanced society where there is no prejudice, no potential for individuals, governments or corporations to use or misuse personal information for reasons unrelated to the purpose for which the information might have been given.

Whenever there is prejudice, there is reason for people to be careful of what information (or misinformation) about themselves is gathered and disseminated.

Whenever there are bureaucracies, public or private, there is reason for people to be concerned about what information (and misinformation) is gathered and held, what decisions are being made that are based on it, and how it's gathered – whether by surveillance or otherwise. Should we not be notified of the existence location of all surveillance cameras, CCTVs and the like, not just those operated by government agencies, as is required by PPIPA?

A surveillance society

In an environment of increasingly sophisticated technology, the availability of affordable surveillance equipment is ever-increasing.

The impact of technology on privacy is significant. It enables surveillance via the internet, CCTV, cameras, through embedded devices in consumables tracking our buying habits and the like.

It is true that law enforcement authorities require sufficient powers of surveillance to enable them to investigate crime. Sufficient checks and balances need to be in place to ensure that surveillance only takes place where the investigating authorities have reasonable cause to believe that a crime has taken place or is about to take place. Judicial oversight is an essential part of those checks and balances.

But quite apart from legitimate purposes for the investigation of crime, surveillance technology is routinely used in NSW by local government, private businesses and individuals for "security" and other reasons. Neighbours have been reported to train cameras on each other to intimidate each other or to use as "evidence" in dispute proceedings. Sydney City Council has a system of street cameras capable of tracking an individual's movements across the city.

It was recently reported in the *Sydney Morning Herald* (18.9.08, Sunanda Creagh "They know where you live: big council is watching you") that an officer of Sydney City Council telephoned an applicant for a parking permit to query his application. She said she could see from a computer satellite image of his home via Council's E-View system that he had off-street parking and asked why, that being the case, he required a parking permit. In fact, the officer got it wrong. She was looking at the wrong property. Fortunately for that applicant, the officer went to the trouble of telephoning him before making a decision to refuse his application. If a decision had been made based on that incorrect information, justice would have miscarried. Although a minor example, it is easy to extrapolate that far more serious miscarriages may occur due to human error in interpreting surveillance information.

It is of concern that, as opposed to Google Street View or Google Maps, an individual cannot at present require a local government authority to remove any aerial image of their property from the E-View systems.

An example of the harm that can come from unwarranted intrusion by surveillance came to the attention of the NSW Council for Civil Liberties by way of complaint from a woman living in a strata unit complex. Some other members of the strata body had observed by CCTV a number of male visitors coming and going from her unit in the evenings. They formed the view in the first instance that she was a prostitute and, later, that she was dealing drugs. Neither was in the slightest way accurate. She was a psychiatrist seeing private patients out of hours and was, on occasion, giving them their prescribed medications.

Privacy legislation must ensure that video and camera images are included in the definition of “personal information” where a person’s identity (or, in the case of

satellite images and the like, the person who owns or occupies the property being captured on camera) can reasonably be ascertained from either the image alone or in conjunction with available extraneous material. It must also ensure that surveillance, not only by government agencies, but also by private individuals and corporations is governed by UPPs.

Separate surveillance legislation?

NSWLRC prepared a draft Surveillance Act, which has not to date been taken up by the NSW legislature. The recommendation of NSWLRC remains that separate legislation of the kind drafted should be introduced to regulate all overt and covert surveillance activity in NSW. At present the only express legislation dealing with surveillance in NSW is the *Workplace Surveillance Act*, which covers surveillance only in a workplace setting and doesn't otherwise cover situations where cameras or CCTVs are located on private property. Accordingly, nuisance is the only remedy for a person whose privacy is breached by acts of surveillance other than in a workplace setting or by a government agency covered by PPIPA and HRIPA.

The danger of separating "territorial privacy" and surveillance issues from other privacy issues is that it takes surveillance out of an established human rights framework. It would be preferable for it to be included in the general privacy legislation, so that it is governed by the same UPPs as other kinds of privacy.

Specific legislation dealing with surveillance technology has not assisted greatly to date. Changes to the Federal *Telecommunications (Interception & Access) Act*, and the *Surveillance Devices Act* via various anti-terrorism enactments have turned laws that were originally designed to protect privacy into ones which authorise substantial invasions.

Deficiencies

We can identify at least two major deficiencies in the laws as existing and as proposed in terms of limiting the growth of surveillance.

1. The existing and recommended exemptions to the privacy principles weaken the protections significantly, especially in relation to government agencies and investigation bodies.

2. Without a legislated cause of action for breach of privacy, enabling individuals to sue for breach of privacy and obtain a raft of remedies including damages and injunctions, the protections offered by legislation will never be adequate in controlling or limiting the growth of surveillance and its impact on privacy.

We need:

- legislation creating a cause of action for breach of privacy.

- the ability to seek an injunction preventing use or continuing use, abuse or gathering of personal information.

- a raft of remedies including correction of misinformation, removal of out of date or incorrect information, financial recompense.

- in relation to surveillance issues, there should be a cause of action for intrusion (eg by closed circuit TV, eTags on goods recording buying habits, radio frequency transmitters embedded into consumables, stalking).
- The tort of privacy needs to be general in terms so it's capable of adapting.
- all new laws affecting human rights – including privacy – being considered should require a human rights impact statement.

Unless and until these measures are taken, there will not be adequate protection and personal information obtained by surveillance can and will be abused.

Exemptions

Public sector

In the public sector there are more than 20 agencies that are partially or completely exempt (NSWLRC paper p17), apart from the exemptions for various private organisations. These have the potential to make privacy legislation practically ineffectual. NSWCCL agrees with the ALRC that exemptions must be limited as far as possible and should only be allowed in limited circumstances on sound policy grounds. They should also be monitored vigorously and regularly.

Recent amendments to the *Telecommunications (Interception and Access) Act* 1979 (including s6AA) gave security agencies access to stored communications without warrant. This has had the probable consequence, whether intended or not, that those agencies can now access, without warrant, people's bank accounts. Electronic versions of bank accounts are available and are probably accessible by virtue of this legislation – that consequence was clearly not discussed when it was introduced, and its potential abuse is obvious. In passing, it might be noted that review of these amendments via a human rights impact statement would have been likely to reveal this potential consequence.

Small business

Exemptions for small business also have to be approached with caution in an age where cheap electronic collection of data and "customer surveillance" is possible. There must be a balance, that is recognised, to ensure the cost to small business is not too onerous, but small business should not have an unfettered right because of their size to use information as they wish. They have access to databases of personal information about their clients, customers, suppliers.

A privacy code for small business must be developed to ensure, among other things, that surveillance be undertaken to collect only such information as is directly relevant to the business and that it be used in accordance with the purpose for which it was collected. Importantly, customers need to be fully informed of the surveillance, and any information gathered ought not to be disclosed to any third party without proper consent.

Political parties

Exemptions for political parties should also be considered carefully. Subject to the constitutional right to freedom of political communication, political parties should be required to comply with privacy principles if they are using surveillance technology.

Media

The media should not enjoy a blanket exemption either. The public interest in having a free press should be balanced against the individual's right to privacy. Sometimes media go beyond what's reasonable and necessary in reporting news and current affairs with the aim being to scandalise and/or titillate and increase sales at whatever cost. Surveillance of celebrities and others by "paparazzi" journalists ought not be protected. A code for the media needs to be developed to ensure protection against unreasonable breaches of privacy.

Intelligence and defence agencies

Exemptions for intelligence and defence agencies such as ASIO, ASIS, Defence Imagery & Geospatial Organisation (DIGO), Defence Intelligence Organisation (DIO), Defence Signals Directorate Office of National Assessments also need to be considered. It is acknowledged that there is a legitimate public interest in allowing such agencies to use surveillance for legitimate purposes. At the same time, however, this must be balanced against the right of members of the community to be protected from unwarranted intrusion, misuse and abuse of any information gathered. For that reason, legislation should enable actions for damages and injunctions for unwarranted intrusions by such agencies.

Information sharing and data matching ought to be carefully monitored and tightly controlled.

Other ALRC recommendations refer to exemptions for agencies with law enforcement functions and other public sector exemptions. ALRC Recommendation 57-4 would enable the use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006. Where credit agencies are using surveillance, this is of concern.

Apparent correlations between data collected and effect is notoriously unreliable, yet it is commonly used in credit reporting. The old example of the 19th Century correlation between incomes of Scottish Presbyterian ministers and the price of whiskey – correlation does not necessarily imply a causal link. General prosperity was the cause of both in that example. For security agencies to rely on correlation surveillance information gathered or held by credit agencies is dangerous and the more information they hold, the more likely it is that mistakes will be made.

Conclusion

The ALRC and NSWLRC have made some sensible recommendations to provide checks and balances for the collection, storage and security of information, but ultimately, surveillance of individuals is allowed. Tighter controls need to be part of the legislation and the legislation must ensure that there are proper remedies available to individuals whose privacy is breached by surveillance activities, whether overt or covert, by public or private corporations or individuals.

With the availability of affordable of surveillance technology, more and more information is being gathered about us in our daily lives. It must be remembered that the more information that is gathered, the greater the risk of mistakes being made and of misuse or abuse of information. Accordingly, the controls on the way information about an individual is used, stored, passed on and accessed by the individual to ensure its veracity need to be carefully framed.

But more importantly, there should be remedies available for breaches of UPPs, whether by exempt bodies or otherwise, to best encourage compliance.

Based in part on NSWCCL submission to ALRC by Stephen Blanks, Secretary of NSWCCL

P:\Us8\ALRC.doc