
Editorial

Privacy is sometimes seen as an old-fashioned value. We give it up all the time for the sake of money, convenience and safety. But there is a big difference between giving something up voluntarily and having it taken away. The outrage felt when privacy is really violated can come as a shock.

Many new technologies pose a huge threat to our privacy.

- Swimming pool change rooms now have to put up signs banning the use of mobile phones because so many now have cameras.
- The internet is used to send viruses that record every website we visit.
- Databases combine information about our tastes and habits that were once safely separate, enabling corporations and political parties to build up a picture of who and what we are.
- Governments are increasingly keen to keep track of our movements and activities with fingerprinting, iris scans and face recognition programs.

Some people make the choice to live without any technologies that make them easy to track. Most of the time this allows them to keep their privacy, but at a substantial cost. Even then they may not be able to escape. For example, legislation making it compulsory to carry an identity card in Britain is likely to allow no exceptions.

Most of us value our mobile phones and internet access too much to go without them for the sake of privacy, but that does not mean we have to accept every creeping intrusion. We need to think hard about what we are willing to give up, and what really matters to us.

The good news is that not all new technologies violate privacy. The Office of the Commonwealth Privacy Commissioner introduces the concept of Privacy Enhancing Technologies such as anti-spyware software (p.4). However, we do not realise how much less privacy we have. "Most of us think our emails are private. But, email is about as 'private' as a postcard," the Privacy Commission notes.

Both the Privacy Commission and privacy activist Roger Clarke refer to the popular TV show *Big Brother*, but they see the program in different ways. The Commission believes the show demonstrates the need for privacy, saying: "After weeks of having their privacy invaded, many contestants appear to leave the show feeling tired, tense, teary or traumatised. Living without any privacy at all is unnatural and difficult. If it was easy, *Big Brother* would have failed from the start."

Roger Clarke sees the program less favourably. He reminds us that the term "Big Brother" came from George Orwell's novel, *1984*, a horrific warning about the future we could face if we do not guard our freedoms, privacy chief amongst them. Clarke says (p.9):

The Y Generation (roughly, people born in the 1980s) don't remember any of those ghastly experiences, when people's freedom to act and speak and think were subjected to tight constraints by powerful governments. They're inheriting a regime that is highly permissive of surveillance of consumers and citizens. The Y Generation is doomed to re-live history unless they use their imaginations and discover that the mass media has trivialised the message, and that loving Big Brother is as serious a mistake now as it was in 1984.

Australian Democrats Senator Natasha Stott Despoja, is similarly concerned that most people are ignoring the dangers to our privacy. She believes part of the problem is that people think the Privacy Act protects them more than it does. She writes (p.14): "The Act contains a range of exemptions. The most outrageous of these is the exemption for political parties, leaving them free to collect, store and act upon highly sensitive information without any regard for privacy. This is a classic case of politicians taking a 'do as we say, not as we do' approach."

Few things are as private as one's genetic make-up. But plenty of people would like to have access to it. Sometimes there may be good reasons, such as police wanting a DNA sample if they have reasonable grounds for suspecting someone of committing a crime.

In other cases there may be less justification. Insurance companies would like to be able to test people for genetic diseases so they can charge higher premiums to those likely to get sick. Many people believe it is not in society's interests to give them this information, but on the other hand it is good for people to be tested, particularly for treatable genetic conditions.

Renowned genetics research Prof Bob Williamson (p.20) points to an example of a win-win solution to the problem of insurance for people at risk of the debilitating genetic disease haemochromatosis: "Australian insurers realised that it is in their interests to encourage people to better health".

Prof Loane Skene (p.23) points out that the solution is not always that simple: "It is important to understand that genetic information is different from other kinds of medical information. Genetic information has two aspects. The first is familial – a mutation exists in a family... The second aspect of genetic information is personal."

The difference is important. Personal genetic information is yours alone, and your rights to privacy over it are high. But Skene adds: "If I am found to have a genetic condition, that diagnosis has immediate implications for my blood relatives". Warning a close relative that they also may have a particular genetic condition may save their life. In the process, however, information that you want kept secret may come out. Plenty of tricky moral dilemmas can result.

Sometimes a little thought about the best ways to use technology can save a lot of heartache. Networked databases can save medical facilities huge amounts of money, as well as assisting in important research. Both aspects can lead to better treatment.

However, Suzanne Dean and Jennifer Luntz (p.27) believe there are profound flaws in the structure of the database used for mental health patients in Victoria, such that initial assessments about a patient remain on the database even if they are subsequently proven to be incorrect, and the information may be accessible far too widely. "Human rights would be advanced and nothing would be lost by having distinct databases for epidemiological and registration information," they conclude.

Worrying about privacy is considered by some businesses to be a drag on their productivity and profitability, but Paul Twomey, CEO of Privacy Solutions Asia Pacific, sees things differently: "Some institutions recognise that their customers' desire for privacy represents an opportunity to increase the trust value of their brands," he says (p.38). Companies that not only protect privacy but also demonstrate they are doing so will win customer loyalty as a result.

Privacy in the workplace is a hot topic at the moment. The Victorian Law Reform Commission (VLRC) notes (p.29): "Privacy in the workplace has changed dramatically in the past 25 years. A boss was once able to keep an eye on employees by personally watching them work, but now there are many more ways to monitor worker performance."

The VLRC has recently held an inquiry into the topic, and concluded: "Employers have a legitimate need to protect their business and ensure a safe workplace for workers, and the Commission's recommendations will attempt to provide a balance between employers' and workers' interests."

How those interests should be balanced is an area where employers and unions disagree. David Gregory of the Victorian Employers Chamber of Commerce and Industry says (p.31): "Employers are responsible for ensuring that acceptable standards of behaviour are observed in the work environment". Sometimes this requires employers to monitor their staff in ways they may not like.

The Victorian Trades Hall Council believes: "Workers

have a right to privacy in the sense that their privacy should not be invaded unless there is a compelling and specific reason". They consider these reasons rather less common than the employer associations.

By the way, if you are wondering why so many of the authors in this edition represent Victorian organisations it is because they were the ones who responded to requests for articles. It is hard to know whether this indicates that privacy is a hotter topic in Victoria than elsewhere.

Josh Meadows from Privacy Victoria (p.42) notes that many of the tricky privacy questions we face relate to transport. Cars are being marketed that can be tracked by satellite, and there is even a prototype that displays the driver's licence number rather than number plates.

These adjustments to vehicles are marketed as safety devices, and they may offer advantages in this area. However, they also mean that plenty of people can find out everywhere you've been – something that may not seem a problem until you have to explain why you were at the beach when you were supposed to be working. Young people may find it a lot harder to visit boyfriends or girlfriends if their parents don't approve.

Ultimately the greatest threat to our privacy does not come from new technology, although it may speed up the rate of danger. The real threat is from governments that want to control everything we do, and from unscrupulous companies and individuals that want to know more about us than they have any right or reason to.

Most of all the threat is from ourselves if we can't be bothered thinking about what really matters, how much privacy we need, and how we can make technology work for, not against, our right to be ourselves. **Stephen Luntz, Editor**

Broaden Your Knowledge on Issues Like:

- Toxic Waste
- Food Security
- Greenhouse Gas Abatement
- Gene Patenting

Order recent editions you've missed by using the form on the inside back cover or order online at www.issues.control.com.au

