

PRIVACY CONFERENCE SPEECH 26 JUNE 2001

CHRIS MAXWELL, PRESIDENT LIBERTY VICTORIA

I will be talking about personal information and Government. I want to suggest a framework within which we can consider the multiplicity of issues which arise in connection with personal information and Government, and the tension which arises between privacy on the one hand and what is generically referred to as “the public interest” on the other.

Liberty Victoria starts from the proposition that personal information is a personal affair. It is no-one else’s business. If a government agency wants to collect, or store, or disclose personal information, then the onus is on that agency, or the legislature, to establish –

- (a) the necessity for the collection, storage or disclosure; and
- (b) the proportionality between the collection procedure adopted and the end sought to be served.

The International Covenant on Civil and Political Rights refers to –

“the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.”

The phrase “unlawful interference” is important, because if the interference has been authorised by law, then the Covenant provision would have nothing to say about it.

The question, therefore, is what legal framework should exist to determine -

- which interferences with privacy are lawful, and by what means;
- how the information should be stored; and
- what use may be made of it.

If privacy safeguards are to be effective, there needs to be public insistence. If those for whose benefit these rights exist are indifferent, then the rights will be eroded. The technological urgency which those marketing the latest equipment consistently emphasise is such that, if we do not mark out the boundaries ourselves, the technological onslaught will simply continue unchecked.

There are some encouraging signs. First, a survey in the Herald/Sun about a month ago showed that public concern about intrusions on privacy had increased. Secondly, there has been a spate of stories in the press about privacy issues. It is vital that journalists continue to identify and investigate encroachments into privacy.

Collection and storage

There are five key criteria which should govern consideration of whether the collection of particular information, and its retention, are justified and appropriately handled. Those criteria are as follows:

- purpose;
- relevance;
- knowledge;
- security; and
- accountability.

(For those of you familiar with the Information Privacy Principles in the *Commonwealth Privacy Act*, you will recognise that what I am about to say is echoed in various of the principles – and I will make references briefly to them.)

As to **purpose**, the purpose of the collection and retention of information by Government or a statutory authority must be clearly defined and adhered to. (See Privacy Principle 1.)

As to **relevance**, only information relevant to that defined purpose may be collected. (Refer to Principles 1.1(b) and 7.1.)

As to **knowledge**, the person the subject of the information must be made aware of three things, namely –

- (a) the fact that the information has been collected and retained;
- (b) the purpose for which it is collected and retained; and
- (c) the nature and purpose of any possible or intended disclosure. (See Information Privacy Principles 2 and 3.)

As to **security**, the information storage facility must be secure. There must be a guarantee to the person whose information is stored that the storage facility is secure against unauthorised access - for example, by allowing access only through a pin number. (Information Privacy Principle 4.)

As to **accountability**, where access is had to the information there should be a paper or electronic record of that access. If questions arise after the event - who had access? were they authorised? what was the purpose of the access? to whom was that information provided - then the storage facility itself will have the footprint of that access having occurred. (Information Privacy Principle 10.2.)

Secondly under accountability, the person the subject of the information should be able to find out what information is held, should be able to go to the agency in question and say,

“I want to know what you have got on me at the moment. In particular, I want to know if it is up-to-date. I want to know if it is relevant to the purpose for which you are entitled to hold information, and I want to know whether it has been disclosed.”

Now, of course there will be exceptions to the last point - in relation, for example, for law enforcement. If I were told that information about me had been disclosed to an investigating authority, then that would be likely to impede the investigation.

Those five criteria – purpose, relevance, knowledge, security and accountability – apply whether the provision of the information is voluntary or compulsory. For example, if I am asked to participate in a survey for the Bureau of Statistics, my provision of information will be voluntary but I am entitled to know that each of those five requirements is satisfied.

Liberty had a complaint recently from an individual who had been asked by an ABS interviewer to answer a survey about health and the use of medication. The person declined and was given a letter which referred to liability for a fine of \$100 per day for so long as the refusal continued. We are in the process of exploring with ABS how that could have occurred. In fact you cannot be fined unless you have had a formal direction from the Commonwealth Statistician (who has a statutory power to give a direction). A failure to comply with such a direction exposes the person to a fine, but a mere refusal to participate in a survey does not.

Disclosure

The bedrock principle is that information collected for one purpose must not be used or disseminated for any other purpose. Anyone whose information is held by an agency must be able to rely on that guarantee.

Misuse of information will be an interference with privacy, in the terms of the Commonwealth Privacy Act. (See Information Privacy Principle 10.1 and *Johns v. The Australian Securities Commission* (1993) 178 CLR at 408, see esp. 423-4 Brennan J and 435-6 Dawson J.) The public law point is that if a person has a power to require the provision of information for a particular purpose, then it will be beyond that person's power, as a matter of law, to put that information to any other use.

There are different degrees of protection against disclosure. At the highest level is a statutory prohibition on disclosure other than for the purposes of the relevant legislation. The best example is section 16 of the *Income Tax Assessment Act*, which prohibits a taxation officer from disclosing taxation information except in the performance of her functions or the performance of her duties. There are equivalent provisions in the legislation governing most statutory authorities.

At the next level down, disclosure for a different purpose may take place if the person –

“is reasonably likely to have been aware, or made aware, that information of that kind is usually passed on to that person, body or agency.” (IPP 11.1(a)).

That is an objective test. If you can be expected to have known that the holder of the information is in the habit of passing on such information on to another agency, then it is permissible, without your express consent being obtained, for that to occur. In the new private sector privacy principles the same test is put slightly differently (2.1(a)) –

“if the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose.”

Nice questions will arise about what the ordinary member of the community will “reasonably” be expected to know. What judges might think was reasonable, knowing what they do about the way the bureaucratic machinery works, may be quite different from what any given group of travellers on the Flinders Street tram might think was reasonable.

Then there is an exception for disclosure where it is made with actual consent. That kind of consent can either be given in advance, as a general authority, or in response to a specific instance. That is, you are asked whether you will consent to the disclosure of the information for a particular purpose (see Information Privacy Principle 11.1(b).)

Recently Liberty was contacted about a proposed request to respondents to the Census, to consent to the release of the information in 100 years for the benefit of historians and demographers. That seems to me to be a proper request, but it should be a revocable consent, that is, if you give your consent now you should be able to change your mind later.

Then there is an exception for disclosure to law enforcement agencies. The test is one of reasonable necessity. Is the disclosure reasonably necessary for law enforcement?

In our view, that is a pretty soft test. What it means is that, if information about a person is on a record at a government agency, then if it is perceived to be “reasonably necessary for law enforcement”, that information can be given to a law enforcement agency without reference to that person. It is a very low threshold particularly when you have an investigating police officer declaring to the agency official (who knows nothing about the criminal law) that the disclosure is reasonably necessary.

The *Telecommunications Act* has a similar provision permitting the release of telephone call record information to law enforcement agencies where it is “reasonably necessary”. It was revealed in Federal Parliament in April that, in the year 1999/2000, nearly a million pieces of call record information were provided to police under this rubric. That is highly private information. Of course, it is not the content of the conversation but it gives a very good picture of where you have been, who you have been talking to and for how long.

The contrast we would draw is with telephone-tapping which is more intrusive again but which cannot occur without a warrant from the Attorney-General. The case has to be made out through the Attorney-General’s Department and then the Minister before a warrant will be granted.

Before private information is made available for law enforcement purposes, there should be an independent assessment of the justification for the disclosure. The balancing of the

claimed necessity against the presumption of non-disclosure of private information should not be undertaken either by the policeman or by the official who, it can be assumed, is not in a position to evaluate the strength of the police claim. It should be done by a magistrate or someone with that degree of independence.

There is a related issue about police disclosure of information in connection with investigations. Liberty Victoria recently expressed strong views about the publication, first in the “Sunday Age”, of extensive information about a person thought to have been involved in the Tynong North murders of 20 years ago. The Herald/Sun helpfully followed that up, found him, photographed him and published his name and location – all purportedly for his own benefit.

Liberty’s view - and I have written to the Chief Commissioner about this – was that this was an unholy alliance between the police and the journalists, which had the effect of exposing someone who has never been charged to the most gross invasion of his privacy. Likewise, the Herald/Sun carried an appalling front page regarding the “Silver Gun Rapist”, based solely on the fact that he had been interviewed – not charged - in relation to some other matter. The article was written in that vigilante spirit that we see abroad in Britain at the moment, which is very frightening because of what it says about our supposedly civilised community.

It is one thing for police to call for information about a particular unsolved matter. No-one could complain about that. It is quite another for police to feed information to the press about people who have not been charged. (According to the journalist, the “Silver Gun Rapist” material had not come from the police.) Police should be very circumspect in providing information which will be seized by hungry media, given how almost incurably prejudicial that kind of publicity is.

There is an issue about information on public registers like births, marriages and deaths. That is not an issue that has come to Liberty’s attention specifically but, to put it shortly, the concern is that information which has traditionally been public is now available and

accessible electronically. That makes it much easier to gather bits of information about a particular person from different public registers and thus to build up a profile. If you had to do it all by manual searching, you could never have done that.

Investigative privacy

Liberty has been approached by a group of plaintiffs' lawyers who act for claimants for statutory benefits. They are concerned that, as a condition of having a claim investigated, the claimant has to sign a very wide-ranging authority empowering the agency to get access to information from police, taxation, health, and so on.

This invites the question "Is that a free consent? What level of access is it right for the agency to insist on?"

Other privacy issues arise about the types of enquiries that are made by such agencies, intrusive enquiries which may adversely affect personal relationships between the claimant and the person spoken to, eg. the family doctor or the priest at the local church. Then there is an issue about the dredging-up of old convictions and their use in cross-examination of claimants. On the one hand the agency says "We have got public money at stake here, we must weed out bogus claims." On the other hand, there is a very important question about what price the community is prepared to pay.

It eventually comes back, as all these privacy questions do, to an identification of how significant the problem is, and whether the response to it is proportionate or disproportionate.