EMBARGOED UNTIL TABLING OF REPORT IN PARLIAMENT

2 August 2011

Key Recommendations

The Law Commission report *Review of the Privacy Act 1993* contains over 100 recommendations. Many of these recommendations are quite technical. But there are some key reforms that the Commission believes will make significant improvements to the operation of the Privacy Act, the protection of privacy and the balancing of privacy with other interests. This report completes the Law Commission's broader review of privacy law. Earlier reports in the series also made significant recommendations for law reform. In particular, the report *Invasion of Privacy: Penalties and Remedies* (2010) recommended major reforms to the law governing the use of surveillance devices by private individuals.

New tools for the Privacy Commissioner

At the moment, enforcement of the Privacy Act is complaints-driven. People can complain to the Privacy Commissioner about breaches of their privacy rights under the Act. But the Commissioner has only limited powers to take action about breaches of the Act on her own initiative. Such a system is often not well suited to addressing underlying systemic problems. The Law Commission thinks the Privacy Commissioner needs new powers so that she can be more effective in ensuring compliance with the Act.

The report recommends two important new powers for the Privacy Commissioner:

- The Commissioner should be able to issue a notice to an agency that is in breach of the Privacy Act, requiring that agency to take action to bring its practices into compliance with the Act. The agency would have a right to appeal such a compliance notice to the Human Rights Review Tribunal. Such a power would bring the Commissioner into line with the majority of overseas privacy commissioners.

- The Commissioner should be given a power to require an audit of an agency's practices and systems for handling personal information. The Commissioner would only be able to require an audit for good reasons, such as if there are grounds for believing the agency's systems are inadequate to protect privacy, or if the agency handles particularly sensitive information (health information, for example).

Data breach notification

There have been some very high-profile cases, both in New Zealand and overseas, of personal information relating to large numbers of individuals being lost or accessed by computer hackers. Such breaches put people at risk from identity theft and other threats.

The Privacy Act does not currently require agencies that hold personal data to notify people when their information is compromised in this way.

The report recommends that notification should be mandatory in cases where notification will enable people to take steps to mitigate a risk of significant harm, or where the breach is a serious one (for example, because the information is particularly sensitive). Notification should be made to the individual whose information has been compromised, and also to the Office of the Privacy Commissioner.

Streamlining the complaints process

The Privacy Act complaints process is unnecessarily complicated, the Law Commission believes. The Privacy Commissioner currently has no power to make binding decisions on complaints; only the Human Rights Review Tribunal can make binding decisions. The Law Commission thinks it is appropriate that the Privacy Commissioner should continue to focus on settling complaints by conciliation wherever possible.

However, the report recommends changes with respect to those privacy complaints that cannot be settled by conciliation:

- The Privacy Commissioner should be able to decide whether to bring proceedings in the Human Rights Review Tribunal. At the moment, this decision is made by the Director of Human Rights Proceedings, adding unnecessary complexity to the system. The recommended change should make the process simpler, more efficient and easier to understand.

- The Privacy Commissioner should be able to make binding decisions on "access" complaints. These are complaints concerning an individual's right to have access to the information that an agency holds about him or her. Where a person complains to the Commissioner that an agency has failed to provide such access, the Commissioner should be able to make a decision that the agency should release the information. The agency would have a right of appeal.

The Commission also recommends that the Act should provide more clearly for representative complaints – complaints made by a person or body on behalf of a group of individuals. Representative complaints can have a number of advantages over complaints by individuals, including having a higher profile and better addressing systemic failures that affect large numbers of people.

Information sharing

Sharing of personal information between government agencies can be desirable for a range of reasons. Information sharing can help agencies to provide better and more efficient services through coordinated service delivery, to detect wrongdoing, or to take joint action against social problems such as child abuse. However, the Privacy Act is sometimes seen as an obstacle to information sharing. Agencies may be unable to share personal information in compliance with the Act, or they may want reassurance that such sharing is legal. The Law Commission thinks that a new mechanism is needed in the Act for information sharing between government agencies, but that it must include appropriate privacy safeguards.

The report recommends that proposals for sharing of personal information between government agencies should be drawn up as agreed programmes. They should go through a process of consultation, including with the Privacy Commissioner. Finally, they should be approved by Cabinet, providing they comply with criteria that would be set out in the Act. There would be safeguards applying to all information sharing programmes, and all programmes would be required to be published on agencies' websites as well as being listed in a schedule to the Privacy Act. Information sharing programmes would be subject to review by Parliament and by the Privacy Commissioner.

Better protection for personal information sent overseas

Globalisation and technological development mean that it has never been easier to send people's information overseas. An increasing amount of information about New Zealanders is stored with "cloud computing" providers, and the servers holding this information are generally located overseas. Privacy laws in countries to which personal information is sent may be non-existent, or inadequate from a New Zealand perspective.

The report recommends new provisions in the Privacy Act about personal information that is sent overseas. Where a New Zealand agency sends personal information offshore to be stored or processed on its behalf, the agency should remain fully responsible for what happens to that information. In other cases, where an agency discloses information overseas but the information is not to be held or processed on its behalf, the disclosing agency should take reasonable steps to ensure that the information will be subject to acceptable privacy standards. The report also recommends that the Act should give the Privacy Commissioner powers to cooperate with overseas privacy protection authorities.

Better protection against offensive online publication

The internet has been enormously empowering, but its power can also be abused through the offensive or harmful publication online of private information about other people. The Privacy Act covers online information, but there are currently some broad exceptions in the Act that the Law Commission thinks should not apply when the publication is particularly offensive. The report's recommendations to narrow the scope of these exceptions will not apply only to the internet, but they are particularly relevant to online information because it can be viewed and copied so widely.

For example, there have been cases of people posting naked photographs of their ex-partners online without consent. At the moment, the person posting such photographs can claim the protection of a section of the Privacy Act that exempts information collected or held in connection with a person's personal or domestic affairs. The report recommends that this exemption should not apply if the collection, use or disclosure of information would be "highly offensive". The report also recommends an amendment that would prevent others from further using or disclosing such information, even though it is accessible from a "publicly available publication".

Health and safety

Protecting the health and safety of both individuals and the public at large is among the most significant reasons why privacy sometimes needs to be overridden. The Privacy Act already includes some exceptions to the privacy principles for cases where it is necessary not to comply with the principles for reasons of health or safety. Agencies are allowed to

use or disclose personal information in order to "prevent or lessen a serious and imminent threat" to health or safety, even if that use or disclosure is not one of the purposes for which the information was originally obtained.

The report recommends that the word "imminent" should be deleted from the health and safety exceptions to the use and disclosure privacy principles. Sometimes a threat can be very serious, even though it may not occur for some time. Although this may seem like a small change, the Law Commission thinks it would be of considerable assistance to agencies that currently feel they cannot release information in the face of a threat that is real but not immediate. The report also recommends that there should be a new health and safety exception allowing information about a person to be collected from someone other than that person; and that, when people request access to information about themselves, agencies should be able to withhold that information if its disclosure would present serious risks to health or safety.

Do Not Call register and direct marketing

The Law Commission considered whether a Do Not Call register should be set up by law in New Zealand, as has happened in other countries. A Do Not Call register would allow New Zealanders to register their wish not to receive telephone marketing calls, and to have that wish respected by marketing companies. At present, the Marketing Association operates a Do Not Call register, but participation in the scheme by marketing companies is voluntary. The report recommends that the Marketing Association's existing register should be put on a statutory footing, making it mandatory for marketers to respect people's stated preferences. The Law Commission thinks that this change should be implemented through consumer legislation rather than the Privacy Act, however.

The report does not recommend any changes to the Privacy Act to deal with direct marketing generally, but the Law Commission thinks that it may be necessary in future to consider whether the Do Not Call register should be supplemented by a right in the Privacy Act to opt out of direct marketing. The Commission thinks that privacy issues in relation to online marketing (including tracking of people's online activity for marketing purposes), and responses to these issues overseas, should be monitored to see if further action is needed in this area in future. The report also recommends that industry bodies should review the adequacy of privacy protection in existing codes for marketing to children.

For further information on these recommendations see the report:

- *New Privacy Commissioner powers – chapter 6, recommendations R63, R64*
- *Data breach notification – chapter 7*
- *Complaints streamlining – chapter 6, R55–R60*
- *Information sharing – appendix 1*
- *Information sent overseas – chapter 11*
- *Offensive online publication – chapter 2, R10; chapter 4, R45; also discussion of online privacy issues in chapter 10*
- *Health and safety – chapter 3, R12, R22, R30, R31*
- *Direct marketing – chapter 12, R116, R121; also discussion of targeted online advertising in chapter 10*