Submission by the Privacy Commissioner to the Privileges Committee

---

Inquiry regarding use of intrusive powers within the Parliamentary precinct

---

11 October 2013

Privacy Commissioner
Te Mana Matapono Matatapu

Submission by the Privacy Commissioner to the Privileges Committee Inquiry regarding use of intrusive powers within the Parliamentary precinct

Introduction

Thank you for inviting our comments on some of the issues you have encountered during this inquiry.

We understand the Committee is tasked with developing principles for the access and release of information from Parliamentary information and security systems. Our submission, outlined below, is that the Privacy Act framework for handling personal information is a comprehensive and sound platform from which to build an approach tailored to the Parliamentary context.

We have made some comments on general points of principle, before making specific points in response to your questions. We hope that this information assists the Committee.

Suggested approach

1. We suggest that the Parliamentary Service could operate consistently, as far as is reasonable, with the widely accepted and principled framework of the Privacy Act when handling personal information.

2. We suggest that the Committee consider supporting the Law Commission's recommendation that the Parliamentary Service, to the extent of its departmental holdings, should be covered by the Privacy Act (see Law Commission R36, set out in appendix 2 of this submission).

1. Privacy Act as an information handling framework

1.1 The Privacy Act 1993 has wide scope and covers both public and private sectors. It is a general statute and is part of the fundamental human rights statutory framework in New Zealand. The Privacy Act provides individuals with the legally enforceable right to have access to 'personal information' held by an agency about him or herself. The Act also contains protections against unauthorised collection, use and disclosure of that personal information.

1.2 The Privacy Act covers most organisations in New Zealand. However, it does *not* extend, for instance, to:

1.2.1 the House of Representatives,
1.2.2 a member of Parliament in his or her official capacity,
1.2.3 the Parliamentary Service Commission,
1.2.4 the Parliamentary Service, except to the limited extent of employee information (definition of "agency", s2).

1.3 There are similar exemptions for the courts and for Royal Commissions, and for the news media in relation to their news activities, amongst others. The policy behind these exemptions is to ensure the discrete and independent functioning of the legislature and judiciary, and to support the free functioning of the fourth estate.

1.4 There is recognition amongst privacy and data protection commissioners worldwide that privacy laws support democratic processes by enabling individuals to exert some control over the way information about them is handled and by obliging business and government to be open and transparent about information handling practices. These protections are becoming ever more important in an environment where personal information is being collected, stored and shared digitally in unprecedented quantities.

2. Underlying principles

2.1 There are certain underlying principles that are evident in privacy laws worldwide, and that underpin New Zealand's privacy law. These include:

2.1.1 Data minimisation – collect only the information that is necessary

2.1.2 Transparency – be transparent and open about the information that is being collected

2.1.3 Individual autonomy and control – provide the individual with the ability to make an informed choice about what information they provide, or how much information they provide

2.1.4 Access and correction – provide the individual with a right of access to information about him or herself, and the right to seek correction if information is wrong

2.1.5 Clarity of purpose - establish a clear and lawful purpose for collecting personal information, and only use and disclose the information in accordance with that purpose.

2.1.6 Data quality principle – take reasonable steps to make sure that information is accurate before use

2.1.7 Security – take reasonable steps to protect information from loss, misuse, and unauthorised access

2.2 These underlying principles are reflected in the 12 principles set out in the Privacy Act. The privacy principles operate together to provide a framework for good information handling practices. An informal outline of the principles is included in Appendix 1.

3. Twin pillars: Official Information Act and Privacy Act

3.1 The Privacy Act is complementary to the Official Information Act in providing a principled basis for access to and release of information across government. The Privacy Act also extends to business and civil society. Both Acts contain a number of withholding grounds that reflect other competing interests, such as prejudice to the maintenance of the law; prejudice to the security or defence of New Zealand; threats to individual safety; prejudice to commercial position; unwarranted disclosure of the affairs of another individual; legal professional privilege; disclosure amounting to a contempt of court or of the House of Representatives, etc.

4. Disclosing information

4.1 In disclosing personal information to a third party, each business or government agency is responsible for that decision under law and according to its own internal accountabilities.

4.2 The scheme of the Privacy Act anticipates that each agency will consider the purposes for which it is collecting and holding information, and it may then lawfully use or disclose information for those purposes. For example, swipe card information might be collected for security purposes (as it is within the Parliamentary precinct). Disclosing that information to investigate a theft would be consistent with that purpose. By contrast, it would clearly be inconsistent with that purpose if swipe card data were to be released to a marketing company, and that release would be found to be unlawful.

4.3 The Privacy Act also provides a number of exceptions which enable information to be disclosed in a range of other circumstances, similar to those outlined above.

4.4 In considering the release of information it may be of assistance to the Committee to consider general practice outside the Parliamentary environment before considering what additional protections or variations might be necessary for the conduct of Parliamentary business. For example, it is common practice to consult affected individuals directly for their views and on occasion to negotiate conditions of release. The nature and relative sensitivity of the information that is to be disclosed is also relevant. Similarly, there may be consideration given to the circumstances in which the information was collected, whether it was by force of law, or whether it was voluntary.

5. Parliamentary or administrative purposes

5.1 The status of the different types of information held on Parliamentary security and information systems is relevant to deciding what rules should apply, as well as who should be responsible for making decisions.

5.2 An analogy is that the Privacy Act does not cover a registrar's actions as part of court proceedings. Those actions are part of the judicial function of the court.

However, actions of a registrar that fall outside the court's judicial functions are covered by the Act. The distinction works well in practice and does not cause difficulties. Similarly, in the Parliamentary context, it does not seem necessary on the face of it for *all* information held by the Parliamentary Service to be excluded from the general law. Information relating to the functions of Parliament and the House clearly would be exempt, but other departmental holdings could be covered.

6. Extending statutory coverage

6.1 While neither the OIA nor the Privacy Act currently covers the operation of the Parliamentary Service, the Law Commission has recommended that the coverage of both Acts should be extended to do so. In the case of the Privacy Act, the Law Commission has recommended that the Parliamentary Service be covered in respect of its departmental holdings, but not in relation to information that it holds as an agent for Members of Parliament. We support that recommendation. We also note that the Parliamentary Service has itself observed to the Law Commission that it already promotes compliance with the privacy principles, as far as is practicable in the circumstances.

6.2 This issue may be considered in the Government's forthcoming response to the Law Commission's *Review of Privacy*. We suggest that the Committee could also consider supporting the Law Commission's recommendation.

7. Concept of information "ownership" is of limited use

7.1 Neither the Privacy Act nor the Official Information Act is based upon proprietary concepts such as "ownership" of information. An agency that collects and holds information has certain obligations to handle that information well, and those obligations are unaffected by ownership of the information itself. For instance, a business or government agency would commonly own the computer hardware or files in which personal information is held, but that does not change the obligations and rights that exist under the Privacy Act in relation to the personal information itself.

8. Metadata is often personal information

8.1 The concept of "metadata" has been widely debated in relation to this inquiry. There are varying views on the nature of metadata and, therefore, the legal rights that are associated with it. The use of a term like 'metadata' suggests that it is information that is of a unique and discrete type. We do not see this as a particularly helpful description, as it wrongly implies that it is data with no personal associations. Increasingly, it is becoming clear that the micro-level, transactional data that is stored about us can paint a very personal picture of our movements, activities, purchasing, and social engagement. As technology is integrated into our daily lives, the extent of the data collected, and its descriptive power, grows.

When that 'metadata' is about an identifiable individual then it is personal information, albeit of a highly specific and granular variety. It is governed by the Privacy Act in the usual way.

9. Concept of "sets" of information

9.1 The Committee has raised the question of the treatment of different sets of information. The Privacy Act does not specify particular classes or sets of information. Information is defined as personal information if it is information about an identifiable individual. There is recognition, however, that some information will typically be regarded as sensitive, or attract a higher privacy interest; health information or financial information are two examples. It is reasonable to expect that sensitive information will be protected with particular care and that appropriate security standards will be used. Nevertheless, it is the case that seemingly innocuous information can, in certain contexts, prove to be highly sensitive. Location-based information is one example.

Conclusion

We hope that this information is helpful. We would be very willing to answer any further questions the Committee might have, either in writing or in person.

K Evans

Katrine Evans
Assistant Commissioner

11 October 2013

for the Privacy Commissioner,
Marie Shroff

Appendix 1 – Informal outline of the privacy principles

- Personal information should only be collected where it is necessary for a lawful purpose of the agency (principle 1).
- Personal information should usually be collected directly from the subject, and the subject must be told it is being collected, by whom and for what purpose (principles 2 and 3).
- Personal information must not be collected by unfair or unreasonable means (principle 4).
- Personal information should be held securely, using safeguards that are reasonable in the circumstances (principle 5).
- Individuals have the legal right to not only see the information that is held about them, but to seek correction of information that they believe to be wrong (principles 6 and 7).
- Each agency must take reasonable steps to ensure that information is accurate and up-to-date before they use it (principle 8).
- An agency should not hold personal information for longer than is necessary for that agency's lawful purpose (principle 9).
- Information should generally not be used or disclosed in ways that are inconsistent with the purposes for collecting that information (principles 10 and 11)
- A unique identifier assigned by one agency should generally not be assigned by other agencies, and should be carefully controlled

Appendix 2 – Law Commission recommendation relating to the Parliamentary Service

R36 The Privacy Act should apply to the Parliamentary Service, but only in respect of its departmental holdings. Information held by the Parliamentary Service on behalf of Members of Parliament should not be covered by the Privacy Act.

Review of the Privacy Act 1993: Review of the Law Of Privacy, Stage 4; August 2011, page 131(following discussion at pages 127 ff)