Privacy (Information Sharing) Amendment Bill

Submission by the Privacy Commissioner

to the Justice and Electoral Committee

---

23 March 2012

Privacy Commissioner
Te Mana Matapono Matatapu

P/0018 /A279460

1. I support passage of the Privacy (Information Sharing) Bill, as long as all its safeguards for privacy are kept intact

1.1. New Zealanders expect government agencies to deliver public services promptly and efficiently. Flexible information sharing processes can reduce duplication of work and improve communication between agencies, resulting in better services for people.

1.2. It appears that government agencies are currently uncertain about when and how they can share information appropriately. This results in agencies being reluctant to share information even though they can or should do so under the Privacy Act as it stands.

1.3. This Bill will provide agencies with the road map that they need, so they can be certain about what they have to do.

1.4. However, it is vital that New Zealanders can trust government agencies to manage their personal information appropriately. Information sharing can be highly intrusive, if it is done without the individual's consent or for purposes that individuals do not expect. Intrusiveness leads to loss of trust. If people lose trust they will be less willing to share accurate information with the government, or will refuse to engage altogether. So getting privacy wrong will result in the government being less efficient, not more efficient.

1.5. This Bill provides strong, practical privacy safeguards so people can be certain that the government is acting as a trustworthy steward of their information.

1.6. In summary, I consider that the information sharing provisions in the Bill will let government agencies share information more flexibly but at the same time safeguard the privacy of individuals. I will be monitoring proposed information sharing agreements carefully to make sure that the balance remains appropriate in practice, as well as in theory.

1.7. I also support the change to the "serious and imminent" threshold for disclosing information when there is a reasonable belief that someone is at risk. However, I am conscious that there is a potential for the lower risk threshold to be misused. I will therefore be carefully monitoring its operation through complaints and enquiries, and will report if unexpected problems start to emerge.

2. This Bill directly affects the relationship of trust between citizens and the State – so it needs to be right

2.1. The Bill makes significant changes to how government agencies can use the personal information of New Zealanders, but it also underscores the fact that government must be a trustworthy steward of the information given to it.

2.2. The Bill comes before Parliament at a time of significant changes in data processing technology and practice. These changes have facilitated the collection, analysis and transmission of information in large databases by both the public and private sector. We are now able to share information more efficiently and more cheaply than we could do before. It is important to use the opportunity that the new technologies provide to improve government processes. However we also need to manage the privacy risks that can and do arise.

2.3. The information sharing provisions of this Bill are part of that wider context of technological change. As the Law Commission stressed in its Review of the Privacy Act, a cautious and well-regulated approach is necessary.

3. There are risks to privacy in the information sharing environment that need to be addressed

3.1. Examples of privacy risks that can arise through sharing information include:

- errors being passed down the chain of multiple datasets (such as wrongly recording that a person has a criminal conviction) – it may be hard or even impossible for the person concerned to get these errors corrected, and they will also result in badly informed decisions;

- information provided for one purpose appearing in a new and unexpected context, resulting in distress for the individual concerned, and loss of trust in government (for example where an individual has multiple addresses for personal or safety reasons and these addresses are merged);

- information provided within a relationship of trust (for example by a patient to a GP, or to a community-based service organisation) being disclosed to an agency where that trust relationship does not exist;

- increased risk of loss or compromise of sensitive information because it is not accorded the same level of protection by the receiving agency as it was by the providing agency (for instance an NGO's funding agency mistakenly emailing the NGO's client information to a third party).

3.2. It is important to note that those risks exist now – they are not risks that arise simply as a result of this Bill. For example, there are many information sharing provisions in other statutes, some of which override the Privacy Act, are open-ended and unclear for the public, and lack basic privacy safeguards.

3.3. In my view, it is vital to create a more consistent framework for sharing personal information, in which the privacy risks are properly identified and managed. This Bill aims to do precisely that, while reducing the current need for lengthy bureaucratic processes.

3.4. My office will need to carefully monitor proposed agreements, to make sure that the privacy risks will be appropriately managed in practice. We will also try to make sure that all agencies are comfortable with the information sharing arrangements, including smaller, community-based agencies.

4. The Bill provides a package of safeguards, all of which are essential

4.1. The framework in the Bill provides a package of safeguards, which are practical, and mutually supporting. The Bill currently represents a fine balance between providing the flexibility agencies are requesting, and ensuring that privacy considerations are given due weight. Reducing the privacy safeguards would unacceptably shift that balance.

4.2. Critical safeguards in the Bill include that:

- Agencies must consult with my office before finalising their agreement, so that independent privacy expertise is brought to bear on the agreement;
- I can publicly report on any privacy matters arising from the agreement, so that the public is appropriately informed about what is happening;
- As the public watchdog in this area, I can review ineffective agreements and recommend amendment or revocation;
- Lead agencies must report regularly and publicly on the operation of their sharing agreements, so that they are fully accountable for what they are doing; and
- The relevant Minister must be able to advise Cabinet that the benefits of sharing information under the agreement are proportionate to the public service being facilitated and that privacy will be adequately protected.

4.3. Each of these safeguards is mutually supporting, for example:

- The requirements on the Minister in section 96K ensure that privacy considerations are given due weight in Cabinet's decision-making – but the Minister will only be able to fulfil this duty if the agencies have done their privacy analysis correctly;
- Regular reporting on the operation of agreements allows me to highlight any unexpected privacy problems that arise once the sharing arrangement is in operation – and the power to review agreements then ensures that those problems will be addressed.

5. "Serious" rather than "serious and imminent" – a justifiable change, but one that needs to be monitored

5.1. Changing the threshold for use and disclosure of information about serious threats is a significant step. However, agencies need to feel more confident that they can share information where this is necessary to prevent serious harm, and therefore I support this change.

5.2. Even where sharing information is clearly permitted by the Privacy Act, and highly desirable (for example in situations where children are at risk) agencies sometimes do not share that information because they feel uncertain about whether they can do so.

5.3. For instance a GP may have serious concerns about a child's safety with a non-custodial parent, and may wish to tell the other parent. At the moment, the GP may feel uncertain about disclosing the information because it is not clear enough whether there is an imminent risk to the child. This uncertainty puts the GP in a difficult situation, and does not address the risk to the child.

5.4. Changing the threshold should remove the problem by allowing a common-sense balance between likelihood of risk, urgency, and the severity of the possible consequences.

5.5. However, this amendment should not be taken as an invitation to disclose any and all information tangentially related to a risk, no matter how slight. If the new threshold is misused, this could in turn lead to considerable harm to people (for example people failing to go to a doctor for medical treatment, for fear that information will be passed on to others).

5.6. Considered judgment will still be necessary in each situation, particularly where agencies wish to disclose sensitive and confidential information. Ethical obligations will also still apply.

5.7. I will be monitoring the application of the new risk threshold carefully, through our complaints and enquiries, and will report if there are any problems with its operation in practice.

5.8. On 29 February 2012 I released a proposed amendment to the Health Information Privacy Code. This amendment would change the threshold for disclosure or use of health information about serious threats, to mirror the provisions in this Bill.

5.9. Public submissions received during the formal consultation process for the amendment will help me gauge whether there are concerns from health consumers and within the health sector.

5.10. The proposals to modify the threshold for risk in the Health Information Privacy Code would not be implemented unless Parliament passes the equivalent provision in this Bill into law.