

2 July 2010



Professor John Burrows  
Law Commissioner  
Law Commission

POST P.O. Box 11-881, Wellington, New Zealand  
PHONE +64 4 472 1600 or 0800 101 151  
FAX +64 4 495 2115  
EMAIL [office@internetnz.net.nz](mailto:office@internetnz.net.nz)  
WEB [www.internetnz.net.nz](http://www.internetnz.net.nz)

**Re: Review of the Privacy Act 1993**

Dear Professor Burrows,

Thank you for jointly organising the two Privacy Roundtables on 21st and 22nd June with us to provide for detailed discussion on Internet-related aspects of the review of the Privacy Act. Our thanks to you and the review team also for participating and providing valuable insights.

We have summarised the issues discussed in the attached document insofar as they relate specifically to the review of privacy law. Hopefully, these will be of value to the review team in the current Stage 4 work.

In addition, feedback from participants has been highly positive about the value they got personally from considering multiple perspectives on the complex and wide-ranging privacy issues that the Internet presents.

Regards,

A handwritten signature in black ink, appearing to read "Vikram Kumar", with a horizontal line underneath.

Vikram Kumar  
Chief Executive

## **Review of the Privacy Act: summary of Internet-related issues**

### **Contracting out of privacy law**

It is not clear what aspects of privacy law people can “contract out” of, e.g. by agreeing to terms and conditions online. While it seems it is not possible for people to knowingly or unknowingly contract out of some privacy principles, e.g. Principles 6 and 7 regarding access to a person’s personal information and its correction, it may be possible to do so in regard to other principles. An amended Privacy Act should make this clear.

### **International harmonisation**

There is recognition and acceptance that terms, scope and applicability of the Privacy Act should take into consideration the privacy laws of other jurisdictions, in particular OECD countries. While this may impose some constraints, for example in clearer definition of personal information, the benefits from international harmonisation outweigh the limitations imposed.

### **Informed consent online**

The application of many of the privacy principles can be modified or not applied with the consent of the person. Getting informed consent is therefore vital. This is against a backdrop of common business models online that depend upon targeted advertising and encouraging people to share more and more personal information. Additionally, it can sometimes become difficult for a person to know what and when personal information is being collected online.

The general practice online is to have lengthy, complex, and often overly legalistic terms and conditions that people have to accept if they want a particular online service. This creates information asymmetry and sometimes reflects power imbalance. Terms also often do not fully explain subsequent aggregation or mining of personal information.

One possible solution is a “privacy commons” as below. Another is for the Privacy Commissioner or independent bodies in New Zealand to facilitate a process of creating model terms and conditions online with some standardisation of content, layout and terms.

Particular attention has to be paid to obtaining consent from children and young adults online as well as the application of the provisions of the Bill of Rights Act.

### **Privacy Commons**

Similar to Creative Commons for copyrighted material, the notion of a Privacy Commons is an idea that the Privacy Commissioner or independent bodies can look at. Privacy Commons may allow standard icons so that people can tell at a glance what the detailed privacy terms of an online service envisage. It may also allow people to exert more control over how they want their personal information to be re-used.

## **Cookies**

Cookies are one specific way of tracking people online via their browser and providing personalised online services. Continuing a principles-based approach in the Privacy Act will obviate the need to control specific techniques such as cookies.

## **Section 56 and disclosure**

Section 56 currently deals with the collection and holding of personal information by individuals (as an “agency”). The growing popularity of social networking has seen vast amounts of personal information about other people covered under Section 56 being disclosed online. However, disclosure is not covered under Section 56. Amending this Section to provide for disclosure too will provide greater certainty to people’s everyday activities.

## **Aggregation of personal information**

Advances in technology, including the Internet, has made it much easier to collect disparate personal information about people which, in the aggregate, presents significant privacy issues. Agencies disclosing personal information must therefore be required to take this into account and take reasonable steps to ensure that the aggregate impact has been considered.

## **Clarity regarding publicly available personal information**

There is a need to assess and clarify what’s meant by publicly available personal information when making personal information available online is easy, common and frequently misunderstood. For example, the status of personal information willingly shared amongst what a person thought was a closed group of friends is not clear. It is noted that the general European practice is that personal information publicly available for one purpose cannot be re-used for another purpose. There is merit in adopting that approach in New Zealand.

## **Role of ISPs**

Internet Service Providers (ISPs) are increasingly seen as a policy or law enforcement point. ISPs require safe harbour provisions for providing access to online content. In the same way, the liability of ISPs in regard to personal information and the costs imposed on them needs to be scrutinised. Possibly a privacy equivalent of safe harbour provisions may become increasingly important. The balance between ISPs being able to provide commercially feasible Internet access as a business versus their legal, policy and enforcement obligations is a debate that is likely to frequently occur in the future.

## **Processing of location information**

With the increased usage of smartphones and Internet-based services disclosing and using a person’s location, there will be increasing attention on collecting, storing and processing information about a person’s location. This is both for location at a point of time as well as aggregated data. This requires consideration of introducing new offences such as tracking a person without consent. In addition, any authorisation obtained should be periodically re-affirmed by the person to minimise the potential harm from consent given unknowingly or mistakenly.

## **Data breach notifications**

Notification of data breaches leading to loss of personal information should be mandatory. However, the success of mandatory data breach notifications depends upon getting a range of detailed parameters right. There was support for a two-step introduction process. Further details about this are in InternetNZ's submission to the Law Commission of 4 June 2010<sup>1</sup>.

## **IP address as personal information**

Whether or not a person's IP address is personal information or not depends upon the specific circumstances. It is therefore appropriate for privacy law to not specify whether or not an IP address is personal information. At the same time, it is noted that there are increasing reasons for linkage between an IP address and an identifiable individual. Therefore it may well be that at some point in the future an IP address will generally be considered personal information. Similarly, a MAC address (unique identifier of a network device), particularly if associated with a physical location, may in practice change from being merely a serial number of a device to personal information. Other static identifiers will become increasingly common as the "Internet of things" evolves and sensors collect, store, process, and transmit information about people.

## **Anonymity online**

It is very difficult, and far more so than most people think, to be anonymous online. For example, unless special protection techniques are used, it is possible to uniquely identify website visitors simply from the combination of information freely available from their browsers. The issue of anonymity and pseudonymity, both online and in the physical world, will always be a balancing act between the need to promote free expression with law enforcement against criminal activities. The Privacy Act currently has got the balance about right.

## **Reporting crime and privacy**

It is noted that many people are apprehensive about breaching the Privacy Act if they report a possible crime, both online and in the physical world, even though this is not in fact true. A public campaign that emphasises the legal position and encourages people to report crime is recommended.

## **Identity crime and the Internet**

Perceptions that the Internet is the main and increasing source of identity theft are not correct. Online service providers have created authentication systems based on shared secrets and identifying people based on a combination of attributes/personal information. This creates a demand for shared secrets and personal information. Breaches of personal information are a supply of such information and mandatory notification of data breaches a necessary response. Breaking this cycle requires better real-world identity proofing processes and reducing the dependence of such processes on "secret" personal information.

---

<sup>1</sup> Copy of submission is at

[http://internetnz.net.nz/system/files/submissions/Submission\\_on\\_Issues\\_Paper\\_of\\_Law\\_Commission\\_review\\_of\\_privacy\\_law.pdf](http://internetnz.net.nz/system/files/submissions/Submission_on_Issues_Paper_of_Law_Commission_review_of_privacy_law.pdf)

## **Jurisdiction issues**

The Internet is a global network and brings with it all the complications of inter-jurisdictional privacy issues. Cloud computing and the popularity of overseas online services increases the offshore flow of personal information subject to the laws of multiple countries. Jurisdictional issues are likely to become more frequent and more complex. Privacy Commissioners working with their global colleagues therefore needs to be further supported. There is also a need to review Section 10(3) as it should not be possible for an agency to outsource accountability for the personal information it collects, holds, and processes. At the very least, the agency needs to demonstrate that it took all reasonable steps otherwise Section 10(3) currently has the potential to create a moral hazard in that agencies are absolved from the responsibility of overseas laws when they should have recognised and mitigated the risks of sending personal information offshore.

## **Everyone as a journalist**

The Internet provides everyone with the ability to quickly and cheaply communicate with a global audience. This creates the potential for every person to be “news media” and get protection under the Privacy Act for disclosing personal information. On the other hand, this protection is neither clear nor counter-balanced by oversight of regulatory bodies. This is part of the larger issue of reviewing news media in the Internet age.

## **Focus on individuals**

The notion of personal information under the Privacy Act is largely in relation to an individual, though there are exceptions such as Section 56 as previously noted. This focus on the individual runs into challenges in some cases such as the Māori notion of collective identity and collective personal information. It also runs into challenges when considering the personal information of families and other collections of people. In these cases, consent can become an issue as well as the concept of harm which are essential ingredients of the Privacy Act.

## **Reasonable belief under Principle 11**

Principle 11 prohibits an agency from disclosing information unless it has reasonable grounds to believe that the listed exceptions are applicable. There are two issues with this. Firstly, Principle 11 is essentially a prohibition, not an enabling provision but is sometimes treated as such. Secondly, reasonable grounds are open to differing interpretations between the requestor and agency. It is therefore recommended that some further guidance around this principle be issued.