Australian Privacy Foundation

Comments on Productivity Commission Issues Paper on Performance Benchmarking of Australian Business Regulation

General comments

1. The Australian Privacy Foundation advocates robust privacy regulation that ensures the best outcomes for privacy protection while minimising unnecessary costs to business, government and the wider community. This means nationally consistent legislation covering all sectors, with simple enforcement mechanisms and good education and prevention strategies.

2. The current privacy regime falls far short of this. The responsibilities on business to protect privacy vary according to the location, size and type of business and also whether it performs work under government contract. A business in one jurisdiction could be subject to two or more privacy laws while the same type of business in another jurisdiction may be subject to none.

3. It is clearly better and easier for all businesses to comply with nationally consistent law than a variety of slightly different laws that apply in different ways and sometimes overlap.

Compliance is not always a 'burden'

4. The terms of reference and issues paper characterise the need for business to comply with the law as a 'burden'. We object to this on two grounds.

5. First, compliance with the law is a responsibility - an obligation to the community. If a regulatory 'burden' on business is lifted, the cost to the community as a consequence must be considered as it may be greater. For example, businesses have an obligation to comply with laws designed to protect the environment. The salient issue is not that the business bears a 'burden' but that the cost to the community of industrial pollution if environmental regulations did not exist, or were weakened, would be too great to bear. The study must not simply assume that any regulation of business must be avoided or minimised, regardless of the cost to the community.

6. Community interests should be put first because they apply to everyone in the country, regardless of any specific business sector or size or governmental jurisdiction. They must be the first level of benchmark that should be supported and not harmed by business/commercial or even government activity.

7. Second, compliance with the law can improve business outcomes and reduce costs. A major driver for the recent expansion of privacy legislation has been the need to engender community trust in conducting transactions online, to enable e-commerce to grow. This was explained in the Explanatory Memorandum to the Federal Privacy Amendment (Private Sector) Bill:

> The Australian public has expressed concern about doing business online, and this concern could frustrate the growth of electronic commerce. The Government acknowledges that user confidence in the way personal information is handled in the online environment will significantly influence consumer choices about whether to use

> electronic commerce. Any business demonstrating that it will protect the privacy of its customers will therefore gain a competitive advantage. Similarly, a country that can demonstrate it protects its citizens' privacy will have an advantage over those countries that do not.[1]

What this means for privacy regulation

8. Privacy is a fundamental and universal right without which individuals cannot exercise freedom of speech and association. It is also intrinsic to human dignity. Like other human rights, it must be available on equal terms to every member of the community. It should not depend on chance, such as where the individual lives, or the size or type of the business, government agency or other entity that has the capability to act in an intrusive way. In our view, privacy must be protected by direct government regulation: nationally consistent legislation that applies to both the public and private sectors.

9. The starting point for benchmarking government regulation should be the values of natural justice, or procedural fairness, which underlie public law: openness; fairness; consistency; impartiality; accessibility; accountability. These values can be adapted to align with the focus of the Commission's study. For example, 'fairness' can incorporate the notion that businesses should not have to meet the cost of complying with measures that do not contribute to achieving the policy objectives of the government regulation;[2] 'consistency' can encompass the aim of harmonising government regulations across jurisdictions so that businesses are saved the cost of complying with arbitrary differences.

10. The present privacy regulatory regime with which businesses must comply is a mixture of direct government regulation, co-regulation and no regulation. Most businesses do not have to comply with any privacy legislation but the delineation can be unclear. Those that do have to comply are subject to different regulations. It can therefore be confusing for business and consumers alike. For example, a business in Victoria may have to comply with federal information privacy legislation, state information privacy legislation and state health privacy legislation, each of which imposes different requirements. A small business in Western Australia may not need to comply with any privacy legislation at all.

11. We reject any presumption that a 'lowest common denominator' approach to privacy regulation imposes less of a 'burden' on business and is therefore preferable.

12. First, the confusing nature of federal privacy legislation is largely due to attempts to carve out exemptions for particular types of businesses and types of personal information. Businesses are required to comply unless they have an annual turnover of less than $3,000,000, as long as they do not provide a health service, deal in personal information, provide services under contract to the Commonwealth government or are related to a larger entity. Those that are required to comply must handle personal information in accordance with National Privacy Principles, unless the information is health information other than health information collected in the course of providing a health service. Employee records are also not protected except

[1] Explanatory Memorandum circulated by authority of the Attorney-General, p1

[2] With regard to the policy objectives of privacy regulation, the Australian Privacy Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy-invasive initiatives can be assessed (see http://www.privacy.org.au/apcc/Charter.html).

in specified circumstances. This complexity adds to the costs to industry associations and individual businesses of identifying and complying with their obligations.

13. Second, the inelegant cordoning off of businesses to which privacy regulation applies has created additional layers of regulation that could have been avoided. The partial exemption of health information from protection under the federal privacy regime has prompted Victoria, New South Wales and the Northern Territory to pass further privacy legislation with which businesses in those jurisdictions must comply when handling health information in any circumstances. The exemption of employee records provided impetus for a review by the Victorian Law Reform Commission into workplace privacy, which has recommended further legislation.[3]

14. Third, the requirements of privacy regulation can lower business costs because many of them align with good business practice generally.[4] For example, privacy laws require organisations not to collect information that is not necessary for their functions or activities. As collecting and storing unnecessary information is costly, compliance with this requirement can reduce business costs. The laws also require that information must be kept securely and protected from unauthorised access, modification, loss or other misuse. Good data quality is essential to any business and, again, compliance with this requirement cannot be construed as a 'burden'.

15. Finally, Australia does not meet the international benchmark of privacy regulation, which was effectively established by the European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. The Directive, with which all EU countries must comply, applies to all personal information, regardless of the size or type of entity that holds it. To the extent that the Australian regulatory regime fails to meet this standard, it potentially creates additional compliance costs for businesses that export goods and services, particularly when they do so via the Internet.

Further comments

16. We look forward to the release of the Discussion Paper and will be interested in providing further comments at that time.

17. However, we are concerned that the timeframe for the study is too short. The terms of reference are broad and complex and it is difficult to perceive how the Commission can produce meaningful and useful recommendations within a few months. We note that the Commission received the reference on 11 August 2006 and was given 12 months to complete it, yet plans to produce a final report by 9 February 2007. We believe that the timetable is unrealistic.

18. Even if the study took the full 12 months to complete, it may be possible only to acknowledge the complexity of the issues and call for further, more targeted, research and consultation. Nevertheless, we would prefer it to the alternative, which is to present a simplistic solution that equates less regulation with better regulation.

---

[3] Victorian Law Reform Commission *Workplace Privacy Final Report* October 2005

[4] For example, Pierrot Peladeau, vice president of Societe Progestacces in Montreal, reported in June 1995 that all 300 businesses and non-profit organisations that had been audited by his firm for compliance with Quebec's 1993 Act Respecting the Protection of Personal Information had gained from implementing data protection either by reducing costs or increasing productivity. *Privacy Journal* June 1995