The Private Sector Amendment to Australia's Privacy Act: A First Step on the Road to Privacy

Alexandra T. McKay

Follow this and additional works at: https://digitalcommons.law.uw.edu/wilj
Part of the Comparative and Foreign Law Commons, and the Privacy Law Commons

Recommended Citation
Available at: https://digitalcommons.law.uw.edu/wilj/vol14/iss1/9

This Comment is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington International Law Journal by an authorized editor of UW Law Digital Commons. For more information, please contact cnyberg@uw.edu.
THE PRIVATE SECTOR AMENDMENT TO AUSTRALIA’S PRIVACY ACT: A FIRST STEP ON THE ROAD TO PRIVACY

Alexandra T. McKay†

Abstract: Global and national transfers of personal information and data protection laws meant to regulate such transfers will have a significant impact on the growing Internet. Yet vastly different philosophies on how to protect individuals’ personal information from theft or misuse by the private sector have led to very different regulatory models throughout the world. In the industrialized world, the European Union’s approach, a universally applicable, comprehensive data protection law, occupies one end of the regulatory spectrum, while a self-regulatory scheme like the United States’ stakes out the other end. Australia’s Private Sector Privacy Act Amendment (“2000 Amendment”) lies somewhere in between. Australia’s 2000 Amendment has been called “co-regulatory” or “light touch” regulation partly because it was meant to allay citizens’ increasing privacy concerns, yet not impose a significant regulatory burden on industry.

Australia’s Private Sector Privacy Bill was touted as an innovative compromise between costly state regulation and ineffective self-regulation. However, some of the concessions made in the name of flexibility and de-regulation have resulted in a weak regulatory scheme that produces inconsistent and ineffective information privacy protection. In particular, the small business exemption and the limited enforcement mechanisms weaken the 2000 Amendment so much as to call into question whether Australia’s information privacy law is merely a baby step away from self-regulation rather than a happy medium on the regulatory scale. If the 2000 Amendment is to provide Australians with the substantive privacy protections it sets forth, legislators should fix two flaws in the next round of private sector privacy regulation. First, they should close or phase out the small business exemption. Second, in order to give effect to the substantive provisions of the Amendment, the law should allow more effective enforcement by using a system of appropriate penalties that escalate according to the degree of non-compliance. These changes would provide more thorough protection of Australians’ privacy, yet would not reduce the benefits derived from the “co-regulatory” model.

I. INTRODUCTION

The advent of the Internet and flourishing of electronic commerce have created opportunities as well as perplexing problems. Data is more easily obtained, stored, transferred, and used than ever before.1 Individuals’ personal information is gathered with ease and is considered economically

† The author thanks Professor Jane Winn and the Pacific Rim Law & Policy Journal staff for their comments and support.

1 Jeff Sovern, Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information, 74 WASH. L. REV. 1033, 1035-37 (1999).
and socially valuable.\(^2\) At the same time, in the last ten years, electronic communication and the World Wide Web have enabled businesses to globalize while expanding their markets and operations. Information gathering and globalization have caused a complex problem to emerge: how can the world harmonize data protection laws so that businesses and organizations can take advantage of foreign markets? At the heart of the problem is the fact that the approach to information privacy varies significantly around the world. In the European Union ("E.U."), the Data Protection Directive sets forth a number of principles related to the collection of personal data, granting to individuals what are essentially extensive rights to information privacy.\(^3\) This Directive prevents data transfers to countries that do not have equivalent data protection.\(^4\) In contrast, U. S. Law grants no official, or unofficial, right to information privacy.\(^5\) Though sectoral U.S. privacy laws target certain industries,\(^6\) efforts to enact generally applicable data protection legislation have been fruitless, as industry has come to rely upon the relatively free exchange of information to conduct business. Instead, businesses are expected to self-regulate their data protection practices.\(^7\)

In the middle of the spectrum between the E.U. and U.S. systems is Australia’s approach, often called a "co-regulatory" or "light touch" approach.\(^8\) Australia enacted a Private Sector Amendment to its Privacy Act (1988) in 2000 ("2000 Amendment"), hoping to strike a balance between Australian citizens’ desire for protection of their personal information, and businesses’ request for flexible guidelines that would not create an expensive regulatory burden.\(^9\)

---

\(^2\) ELECTRONIC PRIVACY INFORMATION CTR. IN ASSOCIATION WITH PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS 2003: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 79 (2003) [hereinafter INTERNATIONAL SURVEY].

\(^3\) See infra Part II.A.


\(^6\) Salbu, supra note 5, at 667.


While it appears that the 2000 Amendment is meant to steer a politically acceptable middle course between the E.U. and U.S. approaches, some aspects of the law weaken it by producing inconsistent and ineffective privacy protection. The first flaw is that it exempts 94% of businesses from its coverage. Second, it does not provide sufficient mechanisms to enforce privacy law. Australia should consider strengthening its private sector privacy law to provide consistent and fair application of its substantive provisions. Because the political process can be slow, now is the time to begin work on the changes that are needed.

To provide more effective information privacy protection, the Australian law should be amended to address its two major shortcomings. First, the small business exemption should be eliminated or narrowed to cover fewer businesses. Second, more extensive enforcement, including a predictable pyramid of increasing penalties for violations, as well as harsher penalties for the most egregious offenders, is needed to ensure the law is followed.

This Comment describes the shortcomings of the 2000 Amendment and argues that they seriously weaken the law. It suggests some relatively simple changes that would address those shortcomings and provide better uniformity in application and enforcement of the law, thereby increasing information privacy protection for Australian citizens.

II. GLOBAL AND NATIONAL STANDARDS REFLECT A WIDE RANGE OF REGULATORY APPROACHES TO PRIVACY PROTECTION

Information Privacy has been the subject of national and international regulation for decades and is becoming an increasingly serious

---


11 See infra Part III.B.

12 This is especially true given that it took years for the first private sector privacy law to pass, despite relatively wide support. Kelly, supra note 8, at 80-85.

13 Privacy is a vague concept covering a vast area of the law. This Comment focuses on information privacy, "which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection.'" INTERNATIONAL SURVEY, supra note 2, at 3. Other types of privacy, such as bodily privacy or domestic privacy, are beyond the scope of this topic.
Because of the globalization of markets and increased use of the Internet, data protection laws are bound to become a major source of contention in the push to increase international commerce. In fact, these laws have already created tension: those who wish to utilize the "boundary free" nature of the Internet are realizing that data protection laws create de facto boundaries that can be just as effective as physical borders. Information privacy is an important national concern as each country tries to bolster confidence in online business by providing data protection that its citizens want, without creating excessive regulatory compliance costs. Information privacy concerns arose long before the Internet, however, and have been the subject of policies and regulations throughout the world for many years.

A. International and European Privacy Laws Set Forth General Privacy Guidelines

In 1980, the Organization for Economic Cooperation and Development ("OECD"), prompted by the increased use of computers to store data as well as the need for international standards of privacy protection, issued Privacy Guidelines ("Guidelines"). These Guidelines articulated fair information practices deemed necessary to protect individuals' privacy. The Guidelines require that data only be used for the purposes for which the individual has given consent. Data is to be protected by reasonable security safeguards, data policies will be open and

---


15 See INTERNATIONAL SURVEY, supra note 2, at 9.

16 The OECD is a global organization of thirty member countries "sharing a commitment to democratic government and the market economy." OECD, About OECD, at http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html (last visited Jan. 14, 2005). The OECD produces publications and statistics as well as instruments, decisions and recommendations. Id. Members include the U.S., the U.K., many western European Countries, Japan, and Australia among others. OECD, OECD Member Countries, at http://www.oecd.org/document/58/0,2340,en_2649_201185_1889402_1_1_1_1,00.html (last visited Jan. 14, 2005).


readily discoverable, and individuals will have the right to access their personal data.\textsuperscript{22}

In 1981, the Council of Europe ("COE") also responded to the rapid expansion of electronic data processing by establishing the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").\textsuperscript{23} Like the OECD's guidelines and the E.U.'s later Data Protection Directive, Convention 108 set out principles that applied to those who gathered personal data. These principles are very similar to the OECD's principles and include how data can be collected, stored, used, and accessed.\textsuperscript{24} COE member states that are contracting states to Convention 108 are bound by its principles.\textsuperscript{25} Whether a country is a contracting party is entirely voluntary.\textsuperscript{26} Though Convention 108 offers good protections, the more recent widespread electronic collection of personal data prompted the European Union to go further.

Influenced by both the OECD guidelines and Convention 108, in 1995 the European Parliament passed the Data Protection Directive ("E.U. Directive").\textsuperscript{27} The E.U. Directive essentially follows the OECD Privacy Guidelines.\textsuperscript{28} It is considered one of the strongest information data protection laws in the world.\textsuperscript{29} The E.U. Directive covers all sectors of E.U. member states' economies and grants strong protection to data containing individuals' personal information.\textsuperscript{30} Individuals are given the right to sue over alleged breaches, and member states have an obligation to form government privacy agencies that will enforce the law and educate the public on privacy.\textsuperscript{31} The E.U. Directive uses the "opt-in" approach to communications whereby an individual must give consent before an organization sends any communications to the individual.\textsuperscript{32} The E.U. Directive also requires non-E.U. countries to have "adequate" levels of

\textsuperscript{22} Id. §§ 12, 13.
\textsuperscript{24} Convention 108, supra note 23.
\textsuperscript{25} Id.
\textsuperscript{26} Id.
\textsuperscript{27} E.U. Directive, supra note 4.
\textsuperscript{28} Id. arts. 5-21.
\textsuperscript{29} Jane E. Kirtley, Privacy and the Press in the New Millennium: How International Standards are Driving the Privacy Debate in the United States and Abroad, 23 U. ARK. LITTLE ROCK L. REV. 69, 74 (2000).
\textsuperscript{30} Salbu, supra note 5, at 668, 689.
\textsuperscript{31} E.U. Directive, supra note 4, art. 22.
\textsuperscript{32} Id. art. 7.
privacy protection if information is to be transferred from the E.U. to those countries. This particular provision has created tension between Europe and other countries whose approaches to information privacy are less comprehensive and stringent. The E.U. Directive has therefore become a benchmark on the global privacy scene.

B. The United States Regulates Information Privacy Through Sector-Specific Laws and Self-Regulation

The self-regulatory and sectoral model of the United States provides a sharp contrast to the European Union's comprehensive Data Protection legislation. The U.S. federal government regulates information privacy in some sectors of the economy (hence the term "sectoral" model). Examples include the Fair Credit Reporting Act, which regulates credit reporting companies' data protection practices, and the Health Insurance Portability and Accountability Act, which regulates health care providers' use of personal health information. The Freedom of Information Act as well as the Privacy Act regulate only the federal government's use of personal information. Other than such sector-specific data protection laws, there is no comprehensive national data protection law in the United States.

Businesses that do not fall under sector-specific laws (including many online and e-commerce businesses) have been encouraged by the U.S. government to self-regulate their use of personal data. Self-regulation has been widely criticized as an inadequate strategy to protect personal data and privacy. The U.S. Federal Trade Commission issued a report in 2000 that questioned the ability of self-regulation to keep pace with the increase in online business and recommended that Congress enact data protection legislation that applied to all online businesses. Members of Congress have introduced over two hundred bills dealing with information privacy

---

33 Id. art. 25.1.
34 George et al., supra note 14, at 736.
35 Salbu, supra note 5, at 691-92.
40 Budnitz, supra note 7, at 860.
41 See generally Budnitz, supra note 7; INTERNATIONAL SURVEY, supra note 2, at 4.
since January of 2001, but none have passed.\textsuperscript{43}

C. Australia’s Private Sector Privacy Law Uses a Co-regulatory Paradigm to Apply Old Privacy Principles to the Private Sector

Information Privacy Protection is not new to Australia. Australia’s government agencies have been required to comply with privacy protection principles for sixteen years. It was only in the year 2000 that the private sector was brought under the umbrella of Australia’s privacy law.

1. The Privacy Act of 1988 Requires the Australian Government to Adhere to Privacy Principles

Australia enacted privacy legislation that applied to government agencies in 1988.\textsuperscript{44} The Privacy Act included a list of Information Privacy Principles similar to the OECD guidelines.\textsuperscript{45} These principles include limitations and guidelines on how the data can be collected, used, stored, accessed, and corrected.\textsuperscript{46} The Privacy Act also established the office of the Federal Privacy Commissioner, an agency responsible for promoting “an Australian culture that respects privacy.”\textsuperscript{47}

2. The 2000 Amendment to the Privacy Act Applies the Privacy Principles to Part of the Private Sector

Towards the end of the 1990s, pressure from diverse interest groups (including businesses, consumers, and government agencies) increased to enact a privacy law that would govern the private sector.\textsuperscript{48} Among the reasons for such pressure were the desire to allay Australian citizens’ privacy concerns in the hopes that they would increase their use of electronic
commerce, the need for national information privacy standards instead of a potentially confusing mix of state laws, and the desire to transfer data to and from Europe where the E.U. Directive requires “adequate” privacy protection measures in the non-European country.

After many false starts and a highly politicized battle, the Privacy Amendment (Private Sector) Bill 2000 passed. It was hoped that the 2000 Amendment would satisfy three goals: 1) increase consumer confidence in Internet transactions, 2) harmonize data protection laws within Australia by preempting different approaches from each State and Territory, and 3) meet the E.U. Directive’s standards so that Australian businesses would not be at a global disadvantage.

The 2000 Amendment took effect in December 2001. The Amendment includes a list of National Privacy Principles (“NPPs”) that apply to the processing of personal information. Those principles include:

50 Kelly, supra note 8, at 80, 83.
51 Id. As of June 28, 2004, the European Union does not consider Australia’s privacy law to be adequate. THE EUROPEAN COM’N, COMMISSION DECISIONS ON THE ADEQUACY OF THE PROTECTION OF PERSONAL DATA IN THIRD COUNTRIES (2004), at http://www.europa.eu.int/comm/internal_market/privacy/ adequacy_en.htm (last visited Jan. 14, 2005). The E.U. cites multiple characteristics of the 2000 Amendment as inadequate including the small business exemption, the exemption for employee records, as well as a number of other provisions of the 2000 Amendment. European Commission, Submission to Standing Committee on Legal and Constitutional Affairs Concerning its Inquiry into the Privacy Amendment (Private Sector) Bill 2000, at 3, at http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf (last visited Jan. 14, 2005) [hereinafter E.C. Submission]. The small business exemption is discussed in detail, infra Part III.A. There are other significant flaws relating to enforcement that the Commission did not mention and that are discussed, infra Part III.B.
54 See Explanatory Memorandum, supra note 49, at 11.
56 Privacy Act, 1988, sched. 3. The National Privacy Principles are almost identical to the Information Privacy Principles of the original Privacy Act.
1) collection, 2) use and disclosure, 3) data quality, 4) data security, 5) openness, 6) access and correction, 7) identifiers, 8) anonymity, 9) transborder data flows, and 10) sensitive information.

There are a few provisions in particular that make the 2000 Amendment "co-regulatory." The first is that the NPPs are only the default standards. Private sector businesses can submit their own privacy codes to the Federal Privacy Commissioner ("Commissioner") and, upon approval by the Commissioner, be subject to their own privacy codes instead of being bound by the NPPs. In order for the Commissioner to approve a privacy code, the code must "[incorporate] all the National Privacy Principles or set out obligations that, overall, are at least the equivalent of all the obligations set out in those Principles." The second co-regulatory provision is that businesses that are exempt from the 2000 Amendment may still opt-in to its provisions by filling out an application form. The Commissioner must keep a registry of businesses that have opted-in to the NPPs.

The third co-regulatory aspect of the 2000 Amendment is not one specific provision, but a set of provisions and policy choices. The 2000 Amendment's enforcement scheme does not follow the "command and control" regulatory model in which the state and/or some private individuals enforce the law in administrative or judicial tribunals. Instead, the 2000 Amendment focuses on negotiation and arbitration to resolve disputes about companies' privacy practices. It directs the Commissioner to hear and resolve complaints brought by the public on alleged breaches of the NPPs or approved privacy codes, and to resolve complaints using conciliatory methods and enforces the law through adjudication.

---

57 Id. at sched. 3.
58 "Co-regulation" is a regulatory scheme in which "industry develops rules for the protection of privacy that are enforced by the industry and overseen by the privacy agency." INTERNATIONAL SURVEY, supra note 2, at 4.
59 Privacy Act, 1988, § 16A.
60 Id. § 18BB(2)(a).
62 Privacy Act, 1988, § 6EA(3). Businesses may opt in to gain favor with consumers by showing a special commitment to privacy or because they have already implemented sufficient privacy protection measures.
64 See Privacy Act, 1988, § 27(1)(e).
65 Id. § 40(1).
conciliation where possible. If conciliation is not possible, the Commissioner can make a formal determination on whether a privacy principle was breached. These determinations are not binding, although the law states that a party may bring an action in Australian Federal Court to enforce a determination. Anyone may bring an action in Federal Court for an injunction against an organization that breached or will breach a privacy principle. The 2000 Amendment also allows a business to name in its approved privacy code an independent adjudicator who will hear complaints of alleged privacy violations, instead of the Commissioner automatically hearing those complaints. In addition, it allows a complainant to request that the Commissioner review a determination made by an independent adjudicator. Like the Commissioner’s determinations, determinations made by independent adjudicators are enforceable in Federal Court. Under the 2000 Amendment, the Commissioner must keep a registry of all determinations made.

The 2000 Amendment exempts small businesses (those with an annual turnover of less than A$3 million) from the new law unless they fit into one of a few categories: 1) the small business provides a health service to individuals and holds any health information; or 2) discloses personal information about another individual to anyone else for a benefit, service, or advantage; or 3) pays someone to collect personal information about another individual from a third party.

The 2000 Amendment requires that individuals be allowed to opt not to receive marketing materials (called the “opt-out” approach). No part of the 2000 Amendment requires a company to obtain consent before collection and use of an individual’s personal information occurs. While a

---

66 Id. § 27(1)(a).
67 Id. § 52.
68 Id. § 52(1B).
69 Id. § 55A. The Court may conduct a hearing de novo on whether the respondent engaged in conduct that interfered with the privacy of the complainant. Id. § 55A(5).
70 Id. § 98.
71 Id. § 18BB(3)(b).
72 Id. § 18BI(1).
73 Id. § 54(1A).
74 Id. § 80E.
75 Annual turnover is “defined to be the sum of the values of all supplies that an entity has made or is likely to make during a 12 month period.” Australian Bus. Register, ABR Help Glossary, at http://www.help.abr.gov.au/content.asp?doc=/content/I 8257.htm (last visited Jan. 14, 2005).
76 Id. § 6D(4).
77 Id. at sched. 3 § 2.1(c)(iv).
78 Salbu, supra note 5, at 662.
79 Requiring consent before collection and/or use is called an “opt-in” approach. Id. at 661-62.
company must tell individuals that it is collecting their information, the NPPs do not require a company to comply with individual’s requests not to collect or use that information.

Many of the 2000 Amendment’s provisions, such as the opt-out provision, have been criticized. Of these, two in particular stand out: the small business exemption and the enforcement mechanisms.

III. THE SMALL BUSINESS EXEMPTION AND LIMITED ENFORCEMENT MECHANISMS OF THE 2000 AMENDMENT COMPROMISE ITS ABILITY TO PROVIDE MORE THAN NEGLIGIBLE INFORMATION PRIVACY PROTECTION

Consumers, non-profit organizations, businesses, and other countries have criticized the 2000 Amendment. Though many aspects of the law are condemned as inadequate to protect Australians’ privacy, the aspects of the 2000 Amendment that will most likely handicap it are the small business exemption and insufficient enforcement provisions.

A. The Small Business Exemption Weakens Privacy Protection

The small business exemption is a particularly unpopular provision of the 2000 Amendment. The A$3 million annual turnover threshold exempts 94% of all Australian businesses that conduct 30% of total business sales. While the small business exemption may have been a politically expedient compromise when the bill was passed, an effective and flexible information privacy law cannot exempt so much business activity indefinitely. The collection of personal information by small businesses can

---

80 A company must take “reasonable steps” to notify the individual of the collection of information. Privacy Act, 1988, at sched. 3 § 1.3.
81 Unless that use is direct marketing, in which case an individual may opt-out. Privacy Act, 1988, National Privacy Principle § 2.1(c)(iii).
82 See Kohel, infra note 83; E.C. Submission, supra note 51.
84 The 2000 Amendment exempts any business with an annual turnover of A$3 million or less from the provisions of the 2000 Amendment, unless a small business sells personal information or is paid to collect it. Privacy Act, 1988, § 6D(4).
85 Privacy Exemption Queried, AUSTRALIAN FINANCIAL REVIEW, Aug. 25, 2000; Dearne, supra note 52; Kohel, supra note 83, at 728-30.
86 See Gunning, supra note 10.
87 See infra Part III.C.
have a great impact on privacy. There is nothing inherent in a company’s size that would indicate its ability or inability to invade Australians’ privacy by misusing personal information. A privacy breach will feel the same to the individual whose privacy was breached whether a large or small company caused that breach.

Consider, for example, identity theft, a rapidly growing crime. Identity theft costs businesses millions, but it also imposes great costs on victims who must spend hundreds, sometimes thousands of hours fixing the problems caused by identity thieves. Victims often run into problems for years as poor credit ratings linger in their credit files. The identity theft problem is only expected to worsen in the foreseeable future. Small, technologically un-savvy businesses that use computers and software to track their customers may be targeted by would-be identity thieves, especially if basic security standards are not in place. Simple measures such as encryption can deter identity theft caused by hacking or security breach attempts from outsiders.

Proponents of the small business exemption may argue that small businesses do not gather or use personal information often and that the exemption in the 2000 Amendment is appropriate. There are two problems with this argument. First, it may be factually incorrect. It is thought that small businesses incorporate cutting edge technological solutions to business

---

88 During legislative deliberation of the bill, the Federal Privacy Commissioner warned that the small business exemption could prevent the Amendment from achieving its goal of increasing consumer confidence in electronic commerce. F.P.C. Submission, supra note 9, at 7.
90 Identity theft encompasses a number of different types of criminal activity and can range from someone illegally using someone else’s credit card, to the theft of an individual’s entire identity to open bank accounts, take out loans, and conduct other business illegally in that individual’s name. AUSTRALIAN NATIONAL CRIME PREVENTION PROGRAMME, ID THEFT—A KIT TO PREVENT AND RESPOND TO IDENTITY THEFT (February 2004), at http://www.law.gov.au/www/ncpHome.nsf/Alldocs/RWP41EA80A3A81A49D8CA256E1A0002A738?OpenDocument&highlight=identity/o2Otheft (last visited Jan. 14, 2005). Identity theft is increasing by more than 50% annually in Australia. Denise Cullen, The Eyes Have It, THE AGE (MELBOURNE), Mar. 24, 2003; 2003 Annual Report, supra note 47, at 9.
91 Identity theft costs Australians four billion dollars (Australian) per year. Cullen, supra note 90.
92 For example, in the U.S., identity theft victims’ out of pocket expenses totaled $1.5 billion from January 2001 through July 2003. Like the U.S., identity theft was also very high in Australia. PRIVACY AND AMERICAN BUSINESS, PRIVACY & AMERICAN BUSINESS SURVEY FINDS 33.4 MILLION AMERICANS VICTIMS OF ID THEFT, CONSUMER OUT-OF-POCKET EXPENSES TOTAL $1.5 BILLION A YEAR (2003), available at http://www.pandab.org/id-theftpr.html (last visited Jan. 14, 2005) [hereinafter Privacy Survey].
needs more slowly than large companies. To the contrary, when the 2000 Amendment was passed, 70% of the Australian Information Industry Association members, who accounted for 80% of high-tech revenues, were small and medium sized businesses. Even four years ago, the argument that small businesses were not electronically gathering personal data was a suspect assumption given the number of small businesses in the information industry. That argument is even less credible today when 96% of Information and Computer Technology businesses are classified as small businesses.

Even assuming small businesses did not in 2000 and do not now gather significant amounts of personal data, the second problem with the proponents’ argument is that small businesses will collect and store personal information in the future. As more and more companies convert records to electronic files and increase the percentage of commercial transactions they conduct electronically, businesses that cannot do so will be at a disadvantage. Such companies will lose business because consumers may find paper transactions cumbersome, or because suppliers can no longer accommodate non-electronic commercial transactions. Small businesses may lag behind large ones in technology implementation, but that should not forever exempt them from taking on the attendant responsibilities of the use of technology.

If the small business exemption remains a part of the Privacy Act, large companies may be driven to exploit it as a loophole to escape its coverage. Conglomerations of businesses that, in effect, are large enough to fall within the 2000 Amendment’s purview, may intentionally escape obligation by categorizing parts of the business as affiliates (where each “affiliate” has an annual turnover of less than A$3 million). While currently there is no evidence that large companies are exploiting the exemption in this manner, they will face increasing pressure to do so if, in the future, small businesses can gain an advantage by using personal data

---

97 Deane, *supra* note 52.
98 Id.
101 See id. at 4.
102 See id. at 244-45.
104 Deane, *supra* note 52.
without adhering to the National Privacy Principles.

Besides domestic privacy concerns, the small business exemption has international implications. The E.U. Commission (“Commission”), through its Data Protection Working Party, listed the small business exemption as a concern in its submission to the Australian Parliament during consideration of the 2000 Amendment. The Commission determines whether non-European Union countries’ data protection is adequate. To date, the Commission has not approved Australia’s data protection law under the “adequacy” standard of the E.U. Directive. The E.U.’s disapproval of Australia’s privacy law has negative implications for the Australian economy. In order to take full advantage of personal data collection in the “information age,” some companies may want to transfer data to and from Europe. This is especially true for companies that have subsidiaries or affiliates in both Australia and Europe. They experience a disadvantage when they cannot transfer personal data freely from Europe.

Even if the E.U. determines that the 2000 Amendment adequately protects personal data, small businesses would still be prohibited from receiving data from E.U. businesses because they are not subject to the 2000 Amendment’s provisions. Even if a small business voluntarily complies with the 2000 Amendment, or the stricter E.U. Directive on Data Protection, there is currently no agreement between Australia and the E.U. that would allow it to transfer or receive personal data to or from Europe.

The small business exemption is not minor. In fact, it exempts a large number of businesses and business transactions. With the increasing use of

---


106 E.C. Submission, supra note 51, at 3.

107 When a third country’s protection is deemed adequate, personal data can be traded to that country from the E.U. E.U. Directive, supra note 4, art. 25.

108 The E.C. Submission of 2001 is the most recent opinion published by the Commission on Australia’s privacy law. Because Australia’s law has not changed, the concerns voiced by the Commission in the E.C. Submission are most likely the concerns that justify its finding that Australia does not have adequate data protection laws.

109 It is very unlikely that the Commission will approve the 2000 Amendment as is given that the Commission raised many concerns about the 2000 Amendment before it was passed that were not and have not since been addressed. E.C. Submission, supra note 51.

109a Id.

110 The U.S. has solved this problem by forming the “Safe Harbor” agreement with the E.U. under which individual U.S. companies can voluntarily comply with the E.U. Directive and then be allowed to trade personal data once the U.S. Department of Commerce certifies them. George et al., supra note 14, at 765.
technology and the rise of data gathering, it could greatly undermine the
ability of the 2000 Amendment to function as it was intended.

B. The 2000 Amendment Lacks Adequate Enforcement Mechanisms

Unlike the small business exemption, which is only one specific
provision of the 2000 Amendment, enforcement is the product of many
provisions of the law. The criticism that the 2000 Amendment lacks
adequate enforcement mechanisms raises practical and theoretical
arguments that surface in the debate about how to regulate effectively and
efficiently.

Australia’s 2000 Amendment relies on a combination of persuasion,
arbitration, and regulatory and judicial injunctions to enforce its provisions.
Businesses are allowed to write their own codes to govern their privacy
practices. The Commissioner’s office conducts outreach and education to
designate private firms on the requirements of the 2000 Amendment with the
hope that, once educated, businesses will comply. The Commissioner
also acts as an arbitrator when individuals submit written complaints about a
company’s alleged privacy breach.

Since passage of the 2000 Amendment, the Commissioner has
received 3044 complaints. The Commissioner made four formal
determinations under the 2000 Amendment, but they all stemmed from
complaints about one company. Because complaints increased by five-
fold after passage of the 2000 Amendment and the Commissioner’s
Budget was only increased to handle twice the pre-amendment number of
complaints, many complainants had to wait six months for a hearing.

112 For example, budgeting and funding choices can greatly affect enforcement efforts.
113 Dearne, supra note 52.
114 To date, three codes have been approved. Fed. Privacy Comm’r, Register of Approved Privacy
116 Privacy Act, 1988, § 27(1)(ae) (Austl.).
118 See Fed. Privacy Comm’r, Complaint Case Notes and Complaint Determinations, at
Case Notes]. The respondent was a company that collected and sold information about tenants to landlords
so landlords could assess and minimize the risks of renting property to particular tenants. Two Tenants’
Unions brought four complaints alleging numerous violations of the Privacy Act. The Commissioner
determined that seven of the alleged violation of the NPPs occurred while two alleged violations of the
NPPs did not.
120 Id. § 62.
121 Id. § 10.
Budget problems also forced the Commissioner to cut back on community outreach and education efforts.122

The NPPs are enforced through the courts and private conciliation sessions.123 Besides the right to file a complaint with the Commissioner, the 2000 Amendment grants citizens or the Commissioner the right to sue in federal court for injunctive relief.124 So far one case has been brought in federal court and relief was partially granted.125 In addition to complaints or lawsuits filed by individuals, the Commissioner can independently investigate an act or practice of a company if the act or practice interferes with the privacy of an individual.126 If the Commissioner finds that such act or practice breaches the NPPs, however, he cannot issue a determination or any penalties.127 The Commissioner investigated 112 matters in the period from July 2001 through June 2003.128 A very small number of the outcomes of these investigations appear in news releases129 or in the Commissioner’s annual report.130

Australia’s “co-regulatory” approach is embodied in its enforcement scheme. Its middle of the road provisions attempt to split the difference between comprehensive state regulation and self-regulation.131 Since the advent of administrative agencies, many commentators have debated whether regulation or deregulation is appropriate and to what extent entities should be allowed to regulate themselves.132 In an influential book called “Responsive Regulation: Transcending the Deregulation Debate”133 Ian

---

122 Id. § 13.
123 Supra Part III.A.
124 Privacy Act, 1988, § 98 (Austl.).
126 Privacy Act, 1988, § 40.
128 Id. at 74-75. The report does not say how many of those matters involved private sector businesses covered by the 2000 Amendment. It did note that there was an increase of sixteen investigations in the 2002-2003 reporting year over the 2001-2002 reporting year. The 2000 Amendment became effective in December 2001.
130 2003 Annual Report, supra note 47, at 74-75.
131 Europe’s Data Protection Directive calls for the creation of a central administrative privacy agency as well as private rights of action in court to seek damages. E.U. Directive, supra note 4. In contrast, the United States allows private rights of action in some of its sector specific laws, but generally relies on market and self-regulation. SCHWARTZ, supra note 5, at 392-94.
133 Id. Ayres and Braithwaite argue that the regulation versus deregulation debate is stale and that a better view is to look at the interplay between state regulation and private orderings. Many other scholars have used Ayres and Braithwaite’s regulatory response model when proposing or discussing the
Ayres and John Braithwaite propose ways in which private regulation and state regulation can supplement and support each other. They argue that lawmakers should seek to find the right balance so that society does not waste resources on excessive regulatory measures that are costly, yet provide no added value in accomplishing legislative goals. Among other things, they introduce the “pyramid” enforcement model, which uses both self-regulation and state-regulation to achieve the most compliance with the least cost. Ayres and Braithwaite’s work is especially useful in evaluating the 2000 Amendment because of its novelty as a “co-regulatory” framework.

The overall enforcement strategy of the 2000 Amendment may induce compliance from many businesses subject to the 2000 Amendment. However, the 2000 Amendment’s enforcement mechanisms are inadequate because they are ill-equipped to deal with repeat violators or with business entities that will not comply with the law because compliance costs more than non-compliance. The 2000 Amendment’s ability to protect individuals’ privacy will suffer in the future unless a few simple changes are made to its enforcement scheme.

1. The 2000 Amendment Has No “Pyramid” of Deterrents

An important element in effective enforcement of a law is that regulatory responses be tailored to match the mindset and behavior of a
given regulated entity.\textsuperscript{140} A regulatory response that uses only punishment will undermine the good will of regulated entities that are motivated by a sense of responsibility.\textsuperscript{141} At the same time, regulated entities that are motivated only by money and will break the law if it is economically advantageous to do so, should be subject to punitive deterrents commensurate with their level of recalcitrance.\textsuperscript{142} Ayres and Braithwaite use the word “pyramid” because the pyramid shape conveys both the kind of strategy used to exact compliance, and how often a particular strategy is used.\textsuperscript{143}

An effective regulatory response pyramid would be built as follows: at the base of the pyramid (the lowest and widest section) are the regulatory strategies the enforcing agency uses most often.\textsuperscript{144} These should be cooperative strategies like persuasion and education.\textsuperscript{145} Because most regulated entities are socially responsible and will try to follow the law simply because it is the law,\textsuperscript{146} a cooperative stance coupled with a strategy of persuasion and education will result in substantial compliance.\textsuperscript{147} If cooperation and persuasion do not work on a particular regulated entity, the agency should move up the pyramid to a stronger, more punitive response.\textsuperscript{148} For example, a warning letter may be the appropriate next step.\textsuperscript{149} As the agency moves up the pyramid, responses become harsher.\textsuperscript{150} The tapered shape of the pyramid shows that the frequency of use of the response decreases as the response gets more and more harsh.\textsuperscript{151} This means that the harshest penalties at the top of the pyramid, for example business license revocation or very high monetary penalties, will be very rarely used.\textsuperscript{152}

\textsuperscript{140} See generally id. at ch. 2. Ayres and Braithwaite argue that agencies do best at achieving their goals when they strike a balance between punishment and persuasion when exacting compliance. Id. at 21.

\textsuperscript{141} Id. at 24. Ayres and Braithwaite argue that a punitive posture on the part of the agency is undesirable because it projects negative expectations, inhibits self-regulation, and may encourage a culture of resistance. Id. at 25.

\textsuperscript{142} See id. at ch. 2.

\textsuperscript{143} Id. at 35.

\textsuperscript{144} Id.

\textsuperscript{145} Id.

\textsuperscript{146} Id. at 19.

\textsuperscript{147} Self-regulation can be incorporated into the pyramid by allowing businesses or industries to form independent investigating or adjudicating bodies, as in the case of the independent adjudicator provision of the 2000 Amendment. Id. at 106. See Privacy Act, 1988, § 18BB(3)(b) (Austl.). Ayres and Braithwaite discuss a model called “enforced self-regulation” where the state monitors and audits industry’s self-regulation. AYRES & BRAITHWAITE, supra note 132, at 101-103.

\textsuperscript{148} Id.

\textsuperscript{149} Id. at 101-103.

\textsuperscript{150} Id. at 35-36.

\textsuperscript{151} Id.

\textsuperscript{152} Instead of “speak softly and carry a big stick” the metaphor could be modified to “speak softly and carry carrots and a number of sizes of sticks, making sure that you have a big stick.” See Hugh Collins,
There are two ways the 2000 Amendment's enforcement strategy diverges from the pyramid model. First, the 2000 Amendment does not require the Commissioner to publish a list of violations and the corresponding regulatory responses. It does not specify what kinds of violations will result in what kinds of penalties, nor does it require the Commissioner or independent adjudicators to publish guidelines. In order for a regulatory strategy to work, those regulated must know what behavior will result in what regulatory reaction. This allows regulated entities to plan, and it is simply fair: people and businesses are entitled to know the consequences of their actions. In addition, the mere publication of the enforcement response strategy, if equipped with a sufficiently harsh response at the top of the pyramid, will arguably result in greater compliance. Those who might exploit the system will be deterred by the punishments at the top of the pyramid. Those who follow the law because of a sense of social responsibility will feel that their compliance is validated, knowing that their efforts to comply will receive support from the government, and that the "bad actors" who try to cheat will receive appropriate punishment.

The second way the enforcement mechanisms stray from the pyramid scheme is that the 2000 Amendment does not provide for a wide range of escalating punishments. The Commissioner is to use conciliation to resolve alleged breaches of privacy. This approach fits the enforcement pyramid model in that the response is to use education, negotiation, and other persuasive tactics as the first regulatory response. The Commissioner may require that a respondent to a complaint cease any actions that invade the complainant's privacy, take action to redress loss or damage suffered by the complainant, or pay money to the complainant to redress loss or damage. There are no provisions, however, for increasing punishment for repeat offenders. The 2000 Amendment also does not allow the Commissioner to bring an action or issue a penalty or sanction independent


153 AYRES & BRAITHWAITE, supra note 132, at 40-41.
154 See id. at 26. A regulatory strategy that sufficiently punishes the cheaters, will support the sense of fairness in those who play by the rules. Id. That sense of fairness is important in preserving voluntary compliance. Id.

155 Privacy Act, 1988, § 27(1)(a) (Austl.).
156 AYRES & BRAITHWAITE, supra note 132, at 35.
158 Id. § 52(1)(b)(ii).
159 Id. § 52(1)(b)(iii). Loss or damage can include injury to the complainant's feelings or humiliation suffered by the complainant. Id. § 52(1A).
of a complaint brought by an individual. In this sense the range of punishments available and even whether or not the punishment applies is very dependent upon the individual complainant. To the extent that privacy means different things for different people, enforcement outcomes will vary. Such disparate results undermine the appearance of fairness that an effective regulatory scheme requires. Furthermore, private businesses appreciate and deserve predictability in the enforcement scheme.

2. The 2000 Amendment Does Not Set Out Tough Deterrents

The 2000 Amendment contains no explicit mention of any harsh deterrents. Under the Pyramid theory, this kind of deterrent would be reserved until other less harsh responses (the lower part of the enforcement pyramid) had been ruled out. Currently, the Commissioner may award only actual damages to complainants. Without the power to fine businesses for privacy breaches that affect many individuals, generalized widespread harms may be very difficult to redress. Complainants can aggregate their cases into a representative complaint, but unless they follow that procedure (and it appears none have, so far, against the private sector), the Commissioner cannot independently issue punishments according to the aggregate effects of a privacy breach. Often, inappropriate disclosures of large databases of personal information result in little to no compensable harm to many of the individuals whose personal information is contained in the database. Punitive awards, which might compensate for such large or egregious privacy breaches, are not available to the Commissioner under the Privacy Act.

---

160 Id. § 52(1).
161 Even a business that blatantly disregards individuals' privacy may receive a light punishment because the complainant was not particularly affected or concerned about a privacy breach.
162 Determining when a specific individual will complain is probably harder than knowing when an agency will initiate an action, especially if the agency has published its enforcement guidelines.
163 AYRES & BRAITHWAITE, supra note 132, at 30.
164 Privacy Act, 1988, §§ 52(1)-(1A).
166 Privacy Act, 1988, §§ 38-39. A representative complaint is called a class action lawsuit in the United States.
167 A privacy breach may significantly damage the reputation of electronic commerce, yet there is no way to adequately address that harm.
168 See Dearne, supra note 52.
Effective enforcement of the 2000 Amendment will also depend on how the enforcing agency, the Commissioner's Office, is perceived. The 2000 Amendment does not allow the Commissioner to issue penalties or sanctions without investigating a complaint. In practice this may not affect most violations since many privacy breaches worth investigating will produce complaints. Instead, this may create a problem of image. An agency charged with enforcing a law should appear to have (and actually have) some powerful deterrents at hand, even if its stance is usually cooperative and conciliatory. In fact, an agency that has the ability to use powerful deterrents is better able to achieve compliance through persuasion and cooperation because its opinion will have force. A regulatory enforcement strategy that uses only cooperation and persuasion cannot be effective, since not all private businesses will follow the law simply because it is the law. An agency, like the Commissioner's Office, that is essentially a moderator of disputes and an educator, cannot provide the punitive deterrent needed to achieve optimal compliance.

Under the 2000 Amendment as currently implemented, the threat of financial sanctions is unlikely to sufficiently deter privacy breaching behavior on the part of businesses motivated only by economic rationality. So far, the Federal Privacy Commissioner has awarded monetary compensation to only one complainant. The damage award in that case was A$1000. Most businesses covered by the act have an annual turnover

---

169 See AYRES & BRAITHWAITE, supra note 132, at 19.
170 Privacy Act, 1988, § 52.
171 Australians have shown that they are very willing to bring their complaints to the Commissioner. After passage of the 2000 Amendment, complaints increased by a factor of five. 2003 ANNUAL REPORT, supra note 47, at 10. Originally, they were expected only to double. Id. at 62.
172 See AYRES & BRAITHWAITE, supra note 132, at 19.
173 Id.
174 See id. at 24. Ayres and Braithwaite cite a 1971 study of the United States Office of Price Administration. Id. at 26. The author of the study concluded that 20% of firms would comply unconditionally with any rule, 5% would attempt to evade it, and the remaining 75% were likely to comply, but only if the punitive threat to the dishonest 5% was credible. Id.
175 See infra Part III.B.4 for a discussion of the Commissioner's role as arbitrator.
176 There are five published case notes interpreting the 2000 Amendment as it applies to the private sector. Complaint Case Notes, supra note 118.
177 Fed. Privacy Comm'r, 2003 - Complaints Case Note 9, at http://www.privacy.gov.au/act/casenotes/crn9_03.html (last visited Jan. 14, 2005). In that case a financial institution accidentally linked complainants' account to a family member's account. Id. The financial institution sent the complainants' financial information to the family member who, upon seeing complainants' financial status required complainants to provide a A$1000 guarantee in relation to financial dealings between complainant and the family member. Id. The financial institution agreed to compensate complainants A$1000. The Commissioner closed the complaint because the matter had been adequately resolved. Id.
of greater than A$3 million. Based on the low risk that the business will be fined at all, and the fact that so far fines have been negligible, an economically rational business that does not feel the need to follow the law simply because it is the law, will not spend much money on improving its privacy practices.

The Commissioner needs stronger sanctions to appropriately respond to unlawful behavior. In addition, availability of highly punitive responses will allow the Commissioner to make full use of the range of enforcement mechanisms, including cooperation and persuasion.

3. The 2000 Amendment Does Not Give Sufficient Rights to Sue in Federal Court

Limited legal recourse further weakens the enforcement of privacy legislation. The 2000 Amendment gives very limited access to the Australian federal courts. Recourse to the court system is available only after the Commissioner makes a formal determination, or to seek injunctive relief. Citizens may have limited rights to appeal a non-determination decision of the Commissioner to the courts under the Administrative (Judicial Review) Act 1977, but section 64 of the Privacy Act (1988) precludes a right of action to challenge decisions of the Commissioner made in good faith. In addition, the 2000 Amendment states that “a determination of the Commissioner... is not binding or conclusive between any of the parties to the determination.”

Even if most parties in a proceeding before the Commissioner will comply with the Commissioner’s recommendations because they are responsible and law-abiding, there is no recourse against cheaters or even very inept actors who fail to properly implement the Commissioner’s recommendations. Allowing the Commissioner, or even a citizen, to enforce orders in court enhances fairness as well as the ability of the Commissioner to keep the base of the

---

178 The small business exemption exempts most of the businesses with annual turnover of less than A$3 million from the provisions of the 2000 Amendment. At the current exchange rate of US $0.77 to A$1.00, the turnover rate is US $2.31 million. *Currency Exchange Rates*, WALL ST. J., Nov. 18, 2004, at C12.

179 Privacy Act, 1988, § 55A (Austl.).

180 *Id.* § 98.

181 No suits have yet been brought under the Administrative (Judicial Review) Act of 1977 over privacy breaches.

182 Privacy Act, 1988, § 64.

183 *Id.* § 52(1B).
enforcement pyramid wide by using fewer punitive measures in most cases.\textsuperscript{184}

The 2000 Amendment’s minimal recourse to judicial enforcement creates two other related problems. First, the majority of privacy disputes are resolved in private conciliation sessions, so the operation of the law is hidden from public scrutiny.\textsuperscript{185} The public cannot discuss and debate implementation of the 2000 Amendment when that implementation is hidden. Furthermore, a failure by Parliament to acknowledge that information privacy is sufficiently important to warrant recourse to the courts fails to legitimate citizens’ information privacy concerns and undermines the notion that information privacy is a “public” issue.

Excessive limits on judicial enforcement give rise to another problem: a potential lack of uniformity in interpretation of the 2000 Amendment.\textsuperscript{186} This is especially true considering there is no required systemic review of the complaint system. In practice, the Commissioner’s resolution of most disputes may indeed be uniform, but uniform dispute outcomes do not lead to uniform interpretation and implementation of the law. If resolutions are not published, or only minimally published, or if costly records requests must be made to the Commissioner to review decisions, businesses’ ability to tailor their privacy codes and practices to accepted standards is greatly lessened. In addition, there is no guarantee that decisions made under the 2000 Amendment are actually uniform. The Commissioner’s Office is a federal agency that educates, enforces, investigates and advises.\textsuperscript{187} Unlike a court of law, its mandate is not to uphold or foster the rule of law or fair process.\textsuperscript{188} Therefore, increasing opportunities to enforce the 2000 Amendment in the court system would promote open and uniform implementation of Australia’s privacy law.

\textsuperscript{184} See Ayres & Braithwaite, \textit{supra} note 132, at 41, for a discussion of the effect of the height of the enforcement pyramid on its shape. A tall pyramid (an enforcement scheme with severe responses available) is also wider at its base; cooperative strategies are used more often.

\textsuperscript{185} See Dean, \textit{supra} note 52.


\textsuperscript{187} 2003 \textit{ANNUAL REPORT}, \textit{supra} note 47, at 14.

4. The 2000 Amendment Overemphasizes Conciliation in the Resolution of Privacy Disputes

The 2000 Amendment requires the Commissioner to settle disputes using conciliation if the Commissioner thinks it is appropriate.189 The debate regarding the respective merits of alternative dispute resolution and adjudication is not within the scope of this Comment.190 A few major points, however, will show why information privacy may be more fairly resolved in adjudicatory settings rather than conciliation sessions arbitrated by the Commissioner. To the extent that conciliation focuses on appeasement or restoration of goodwill,191 it can neglect the substance of the outcome.192 Legitimate value and interest conflicts can become "communication" problems.193 Some scholars argue that certain kinds of disputes—constitutional or public law disputes—are not appropriate for alternative dispute resolution ("ADR").194 Scholars argue that the process of adjudication ensures the proper resolution and application of public values, whereas ADR emphasizes resolution of conflict using non-legal community or individual values.195

Information privacy is not constitutionally protected. However, many argue that privacy is a fundamental human right, the existence of which coincides with humane government,196 and so it may be exactly the kind of "public law" that is well-suited to adjudication.197

Another criticism leveled at ADR is that power imbalances between parties and a lack of procedural safeguards can lead to ill-informed decisions

189 Privacy Act, 1988, § 27(1)(ab).
191 Webster's defines the verb "conciliate" as follows: "to gain (as goodwill) by pleasing acts 2) to make compatible: reconcile 3) appease: to become friendly or agreeable." MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 239 (Frederick C. Mish et al. eds., 10th ed. 1996).
192 See Abel, supra note 190, at 293-94; Nader, supra note 190, at 8.
193 Nader, supra note 190, at 8.
194 Edwards, supra note 190, at 671.
195 Id. at 675-76.
196 OECD Guidelines, supra note 18; International Covenant of Civil and Political Rights, Mar. 23, 1976, art. 17, 999 U.N.T.S. 171 ("[N]o one shall be subjected to arbitrary interference with his privacy.") Some have also pointed out the economic gains created by privacy protection. See generally Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 GEO. L.J. 2381 (1996).
197 Edwards, supra note 190, at 671.
that are less fair or just than decisions produced by adjudicative bodies. Richard Abel, professor at UCLA School of Law and respected legal author, criticizes ADR for improperly neutralizing conflict in heterogeneous societies. He argues that ADR neutralizes conflict by individualizing it: ADR isolates grievants from each other and inhibits perception of common grievances. Isolated grievants are more likely to give up, even though their complaints may be substantial. Finally, ADR’s purported virtues, that it is faster and less expensive than adjudication, may be less significant than its proponents claim they are.

Both the Commissioner and the Parliament should consider these serious concerns about ADR if they contemplate changing Australia’s private sector privacy law. For example, the Commissioner could publish procedural guidelines for complaints. Parliament should consider lessening the emphasis on “conciliation,” increasing rights of action in court, creating procedures for complaints, or all three.

IV. RECOMMENDATIONS

Parliament can incorporate a number of simple measures into the 2000 Amendment to ameliorate the significant shortcomings caused by the small business exemption and inadequate enforcement mechanisms. First, the small business exemption should be eliminated or narrowed. Enforcement mechanisms should be improved by applying increasingly harsh regulatory responses to increasingly recalcitrant behavior, and by allowing the Commissioner to issue harsh penalties for egregious violations. Improved access to the court system would further increase fair and efficient enforcement of the law. Finally, both the Federal Privacy Commissioner and Parliament should consider increasing education efforts to improve Australians’ understanding of data collection and privacy protection.

A. The Small Business Exemption Should Be Closed or Narrowed

First, Parliament should narrow or eliminate the small business exemption. This could be done gradually so that businesses can make use of protocols and systems developed by businesses already subject to the 2000 Amendment.
Amendment. Gradually closing the small business exemption loophole would give small businesses time to educate themselves and the Commissioner time to develop guidelines to assist small businesses in implementing the law. Small businesses that store personal data can and should implement at least basic privacy measures that are simple and inexpensive. To promote fairness and consistency, small businesses that incorporate more technology and data storage into their businesses, should be held to the same basic standards of care as large corporations that have already been using that technology.

B. The 2000 Amendment’s Enforcement Mechanisms Should Be Improved

A number of changes could improve enforcement of the 2000 Amendment. First, the Commissioner should develop and publish, or Parliament should require development of an enforcement “pyramid.” The Commissioner should publish guidelines that show what enforcement responses will correspond to what kinds of breaches or non-compliant behavior. Regulatory responses should increase (become more punitive) in response to continued non-compliance and decrease with compliant behavior.

Second, the 2000 Amendment should be amended to specifically include more punitive deterrents.203 There are many deterrent options available. Adverse publicity can be a harsh sanction because many corporations place a high value on a good reputation.204 Punitive damages can be assessed in response to especially egregious or repeat violations. Recourse to the court system through a private right of action can also be a strong deterrent.205 Business license suspension may also be considered for the most egregious non-compliant behavior. Under a pyramid system these harsher punishments will be used less often than the conciliatory or persuasive responses.

203 Ayres and Braithwaite would say that the height of the pyramid should be increased. See AYRES & BRAITHWAITE, supra note 132, at 41.
204 Id. at 22.
205 Because of business’s fear of litigation, rights of action can be deterrents in and of themselves regardless of the available remedies. Kimberlianne Podlas, The Monster in the Television: The Media’s Contribution to the Consumer Litigation Boogeyman, 44 GOLDEN GATE U. L. REV. 239, 239 (2004); Deborah A. Ballam, Employment References—Speak No Evil, Hear No Evil: A Proposal for Meaningful Reform, 39 AM. BUS. L.J. 445, 447-48 (2002). In order to retain predictability, private rights of action should be limited by specific standards of review and should be available only after administrative remedies have been exhausted.
Third, the 2000 Amendment should include more access to the court system. Judicial review promotes uniformity, increases public awareness, and bolsters the Commissioner's ability to influence businesses' behavior. Though ultimate recourse to the court system is ideal, it is also important to consider why access to the courts was so limited in the 2000 Amendment and why increasing access to the courts after initial passage is more politically feasible. Businesses and free-market enthusiasts often argue that excessive litigation is a main reason for the "ossification" of the administrative process. Those who favor self-regulation and reliance on the market to regulate interactions, argue that such regulation is more efficient. They argue that the extensive procedural requirements of rulemaking and frequent litigation bog down administrative regulation, which in turn increases costs and delay. Finally, litigation is a source of concern to businesses because litigation is expensive and often unpredictable.

In the case of information privacy laws, some of these concerns are reasonable. The public's understanding of technology and data use is minimal. Accordingly, individuals may not have a strong sense of the information privacy they want or need. Some individuals may be very sensitive to use of their personal information and others may not notice or particularly care. It is difficult to set legal standards in this kind of social climate because actions that constitute a breach and the appropriate remedies are not yet clear. Two important points arise from this discussion. First, it is appropriate to use persuasion and conciliation, as espoused currently in the

210 Jeff Sovem, Protecting Privacy with Deceptive Trade Practices Legislation, 69 FORDHAM L. REV. 1305, 1327 (2001). The author cites a number of sources describing consumers' ignorance about business's collection of personal information. Id. at n. 73; Sovem, supra note 1, at 1071-74; see also JOSEPH TUROW, ANNENBERG PUBLIC POLICY CENTER, AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN (June 2003), at http://www.annenbergpublicpolicycenter.org/04_info_society/2003_online_privacy_version_09.pdf (last visited Jan. 14, 2005) (showing that Americans were ignorant about privacy practices in that many mistakenly assumed that a company with a privacy policy would not share personal data).
2000 Amendment, for most disputes because actors on both sides of a transaction will be acting in good faith and honestly trying to do the right thing. Second, as the public, the private sector, and the Commissioner learn more about information privacy in the private sector, it will be easier to create legal standards that can be applied in court. For example, after receiving thousands of complaints\textsuperscript{212} and resolving almost as many, the Commissioner will likely have learned which breaches are minor, which are moderate, and which are major. The legislature should take advantage of the experience and knowledge gained in the last three years to craft fair and predictable legal standards that can be applied in court.

C. Australians' Attitudes About Privacy Should Be Considered When Making Changes to the 2000 Amendment

The Australian Parliament needs to set aside funds to educate consumers about information privacy. Consumers should be educated on typical industry practices as well as potential risks\textsuperscript{213} of the collection and use of personal information. Parliament and the Commissioner also need to be sure that companies notify consumers of the intended uses of their personal information.

Parliament can choose enforcement mechanisms that free up resources to increase public education. Measures to reduce the budget problems faced by the Commissioner's Office would allow the other changes suggested here to have the greatest effect. Industry could be allowed and encouraged to self-enforce (with auditing and oversight by the Commissioner), which takes advantage of industries' expertise to enforce the law more efficiently.\textsuperscript{214} These measures should relieve some of the financial pressure on the Commissioner, who can then increase outreach and education. However, Parliament should also consider expressly allocating more money to educate consumers about privacy. This would serve the valuable democratic ideal of having an informed populace, but also would allow Australians to decide what privacy protection they desire. This, in turn, would remove some of the uncertainty surrounding social expectations of privacy.

\textsuperscript{212} 2003 \textit{ANNUAL REPORT}, supra note 47, at 15.

\textsuperscript{213} Risks include economic risks, such as lost time and opportunities because of identity theft, as well as moral and social risks, as when a person's sensitive purchasing habits are indiscriminately viewable by company employees.

\textsuperscript{214} Public interest groups could also monitor enforcement efforts under a "tri-partism" model which would serve dual purposes of taking some of the burden off the Commissioner, as well as allowing the Commissioner to form cooperative relationships with industry. \textit{See} \textit{AYRES & BRAITHWAITE}, supra note 132, at 54.
Proponents of the 2000 Amendment may argue that Australians achieved the privacy protection they desired, even if it has serious shortcomings. An alternative possibility is that Australians actually wanted stronger information privacy protection, but were willing to settle for the 2000 Amendment because they saw it as a first step in a line of increasing legal protections and because gradual implementation would lower overall implementation costs, or because they were unsure about the current state of data collection. Speculating about the "political will" of the people is difficult, but some analysis of public attitudes provides relevant information. Studies tend to show that consumers do not have a particularly good understanding of personal data collection. In such a political climate, the default should not be to adopt laws with large loopholes and weak enforcement mechanisms. If minimal protection is desired, the substantive portion of the law (the NPPs in this case) should be changed to reflect that desire, rather than rendering the law inconsistent and unfair through exemptions and inadequate enforcement.

V. CONCLUSION

Given the current state of flux of data collection, regulating information privacy is like trying to hit a moving target. Australia's 2000 Amendment was an innovative approach to regulation of an amorphous subject. Yet the small business exemption and its enforcement mechanisms are serious flaws. By addressing these flaws, the Australian government can provide effective privacy protection, while remaining flexible to changing business and citizen needs. Small businesses that are not currently subject to the Privacy Act can benefit from lessons learned while implementing the 2000 Amendment over the last four years. The Federal Privacy Commissioner can act as a resource for businesses' self-regulatory efforts and can persuade and educate them on what is needed for compliance. But government also needs the power to administer punitive responses. A fair enforcement system is cooperative, open, appropriate, and holds sufficiently punitive responses in reserve. When regulated entities believe that regulation is fair, they are likely to cooperate. A system that works mostly by cooperation is efficient and maximizes outcomes for all involved.

The particulars of regulatory schemes are important, but it is also important to have an informed populace. To that end, Parliament should emphasize outreach and education on privacy issues. A scheme that reflects the sentiments of an informed citizenry will be stronger, fairer, and more

---

efficient.

The 2000 Amendment has clear, moderately strong, substantive privacy protection in the form of the NPPs, but these principles are not being given force. Currently, the small business exemption is too large a loophole. The enforcement provisions are weak. In the name of consistency and fairness, the substantive provisions of the 2000 Amendment should be given force. To do so, the small business exemption should be phased out, and the enforcement mechanisms modified to provide appropriate, predictable responses.