Brooklyn Journal of International Law

Volume 27
Issue 2
25th ANNIVERSARY ALUMNI ISSUE

Article 11

2002

The Privacy Amendment (Private Sector) Bill 2000: The Australian Government's Substandard Attempt to Allay Privacy Concerns and Regulate Internet Privacy in the Private Sector

Matthew Kohel

THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000: THE AUSTRALIAN GOVERNMENT'S SUBSTANDARD ATTEMPT TO ALLAY PRIVACY CONCERNS AND REGULATE INTERNET PRIVACY IN THE PRIVATE SECTOR

I. INTRODUCTION

In many nations the individual's right to privacy is recognized as a fundamental human right.[1] Although Australia does not have a constitutionally guaranteed right to privacy, and it is not a member of the European Union ("EU"), the individual's right to privacy is nonetheless accepted as being fundamental.[2] In 1984, Australia adopted the principles embodied in the Organization for Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("Guidelines"), which were incorporated into the federal Privacy Act 1988 ("Privacy Act").[3] The Guidelines regulate the collection, use, and transfer of personal data in the public and private sector, where the handling of such data may create dangers to privacy and individual liberty.[4] The Privacy Act was Australia's attempt to regulate how

1. In the United States the right to privacy is a constitutionally recognized right. In Europe, privacy protection laws have been introduced, or will be introduced in many countries to "prevent what are considered to be violations of fundamental human rights." *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organization for Economic Cooperation and Development (OECD), 20 I.L.M. 422 (1980) [hereinafter *Guidelines*].

2. ANTHONY BENDALL, OFFICE OF THE NEW S. WALES PRIVACY COMM'R, INQUIRY INTO E-PRIVACY: SUBMISSION TO THE SENATE SELECT COMMITTEE ON INFORMATION TECHNOLOGIES 3 (2000), *available at* http://www.aph.gov.au/senate/committee/it_ctte/e_privacy/submissions/sub26-NSWPrivacyCommissioner.doc (last visited Feb. 23, 2002) [hereinafter INQUIRY I].

3. Privacy Act, 1988 (Austl.).

4. *See Guidelines*, *supra* note 1.

personal information is collected, transferred and disposed of in the public sector.[5] Until recently there was no equivalent statute which binds the private sector. However, as an amendment to the Privacy Act, the Privacy Amendment (Private Sector) Bill 2000 ("Amendment"), was introduced into the Australian Parliament on April 12, 2000 and went into effect on December 21, 2001, and as its name points out, the Amendment aims to regulate privacy in the private sector.[6]

The stated goal of the Amendment is to establish a single comprehensive national scheme for the appropriate collection, holding, use, correction, disclosure and transfer of personal information of organizations.[7] The Amendment proposes to meet this goal by balancing the individual's interests in protecting his or her privacy against social interests, such as the free flow of journalistic information and an efficient economy.[8] Even though the Amendment puts a premium on the protection of the Australian citizenry's privacy, it is nothing more than the Australian Parliament's pretextual attempt to meet international standards concerning personal data collection and transmission. Parts II and III of this Note will discuss the historical background which led up to the proposal of the Amendment. Parts IV, V and VI will propose that the means of achieving individual privacy are flawed because the privacy concerns of individuals, and their trust in electronic commerce, are trumped by the interests of business and an efficient economy. In particular, this Note proposes that the interests of privacy succumb to an efficient economy in two fundamental respects. First, the National Privacy Principles ("NPPs") lack

5. HELEN DANIELS, AUSTRALIAN SENATE SELECT COMMITTEE ON INFORMATION TECHNOLOGIES, INQUIRY INTO E-PRIVACY 2 (2000), *at* http://www.aph.gov.au/senate/committee/it_ctte/e_privacy/submissions/sub25-AG.doc (last visited Feb. 23, 2002).

6. Press Release, Office of the Federal Privacy Commissioner Privacy Law for the Private Sector (Dec. 20, 2001), *available at* www.privacy.gov.au/news/01.13.doc. *See also* Attorney General's Department, *A Privacy Scheme for the Private Sector, Introduction of the Privacy Amendment (Private Sector) Bill 2000, at* http://www.law.gov.au/privacy(last visited Feb. 23, 2002).

7. Privacy Amendment (Private Sector) Bill (2000), pmbl., ¶ 3 (Austl.) [hereinafter Amendment Bill].

8. *Id.*

teeth because the regulatory standard they create is weak, and the language is easily manipulated by business organizations.[9] Second, the exemptions in the Amendment, such as the small business exemption, create loopholes through which organizations can freely collect and transfer information without fear of penalization. Thus, the Amendment will not accomplish its goal, and may even have a detrimental effect on Australian electronic commerce in an age when the promotion of an efficient electronic internal economy is vital to an increasingly global and electronic world market. In conclusion, Part VII proposes technology, such as digital signatures, as a consumer friendly way to protect privacy on the Internet.

II. EUROPEAN LEGISLATIVE HISTORY OF THE DIRECTIVE[10]

Advances in computer technology have resulted in the collection and storage of large quantities of individual information or personal data.[11] There are numerous ways in which personal data can be collected when an individual goes online. It is beneficial to explore a few of the ways in which personal data is collected online to help the reader get a better understanding of the subtlety of these collection practices. One means of data collection is the use of cookies.[12] Cookies are tiny data files

9. The Amendment's National Privacy Principles are the result of the Australian Parliament's incorporation of the National Principles for the Fair Handling of Personal Information. The latter are a non-binding comprehensive set of flexible principles concerning use of personal data which business organizations are encouraged to follow. OFFICE OF THE PRIVACY COMM'R, AUSTL., NATIONAL PRINCIPLES FOR THE FAIR HANDLING OF PERSONAL INFORMATION 2 (1999), *available at* http://www.law.gov.au/privacy/ royallnpp.htm (last visited Feb. 23, 2002) [hereinafter NPPs].

10. Although the focus of this Note is Internet privacy, corporations have historically compiled personal information offline as well. "Experts predict that information that has traditionally been stored offline will be stored and accessed online in the near future. And whether online or off, the information collected is often the same." INTERNET POLICY INST., THE INTERNET, CONSUMERS AND PRIVACY, *available at* http://www.internetpolicy.org/ briefing/alderman_kennedy.html (last visited Feb. 23, 2002).

11. Europa, *Data Protection: Background Information, at* http://europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm (last visited Feb. 23, 2002) [hereinafter *Data Protection*].

12. OFFICE OF THE NEW S. WALES PRIVACY COMM'R, INQUIRY INTO E-PRIVACY: SUBMISSION TO THE SENATE SELECT COMMITTEE ON INFORMATION

placed on a user's hard drive that track the sites the individual visits, and can be used to create a record of all the individual's activities on that site.[13] Many websites use this technique, especially sites that offer goods and services.[14] However, cookies are not just used in commercial transactions. Cookies can attach themselves to a hard drive from registrations, surveys, contests and even when an individual has merely clicked on a site.[15] Thus, cookies allow a website to create personalized profiles of each particular visitor tailored to his or her preferences.[16] Another technique which allows website operators to collect personal information are Web Bugs.[17] A Web Bug is a graphic on a web page or in an e-mail message that is designed to monitor who is reading the web page or e-mail message.[18] Although Web Bugs are a graphic, they are usually invisible because they are only 1-by-1 pixel in size, and they are less detectible than cookies.[19]

Due to the rapid increase in technology facilitating the collection of personal data and the amount of data collected, many nations have passed legislation aimed at protecting the individual's fundamental right to privacy.[20] Dating as far back as

---

TECHNOLOGIES, (2000), *available at* http://www.aph.gov.au/senate/ committee/it_ctte/e_privacy/ submissions/sub15-OFPC.doc (last visited Feb. 23, 2002) [hereinafter INQUIRY II]. *See also* Graham Greenleaf & Roger Clarke, *Privacy Implications of Digital Signatures* (Mar. 10, 1997), *at* http://www.anu.edu/au/people/Roger.Clarke/DV/DigSig.html [hereinafter *DigSig*].

13. *See* INQUIRY II, *supra* note 12, at 3.

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.* at 4.

18. *Id.*

19. *See* INQUIRY II, *supra* note 12, at 4.

20. This is especially true among Member States of the E.U. who have acted in response to Council Directive 95/46. Europa, *Data Protection: Status of Implementation of Directive 95/46*, *at* http://europa.eu.int/comm/internal_market/en/media/dataprot/law/impl.htm (last visited Feb. 23, 2002). For example, ten countries have either wholly adopted the Directive, partially adopted the Directive or passed separate legislation that satisfies the requirements of the Directive. *Id.* Among the nations who have implemented the law are Belgium, Austria, Portugal and Sweden. *Id.* Denmark has partially adopted the Directive by amending its Civil Registration Act, which came into force in late 1998. *Id.* However, not all nations have implemented

the 1970's, several Member States of the EU have passed such legislation.[21] The collection and misuse of personal data has also been an area of great concern to international organizations.[22] In 1980, the OECD created the Guidelines to reconcile national privacy legislation with fundamental privacy rights, while simultaneously preventing interruptions in international flows of data.[23] In response to privacy concerns relating to collection, use and transnational flows of personal data in Europe, the EU passed a directive based on the Guidelines. The EU mandates that personal data be properly collected, distributed and protected through Directive 95/46 of October 24, 1995.[24] The Directive took effect on October 25, 1998 and is "designed to safeguard the privacy of European citizens in the face of increased personal data collection, storage and sharing by corporations."[25] The Directive applies to the processing of personal data, wholly or partly, by automatic means, and to the non-automatic processing of data which forms part, or is intended to form part of a filing system.[26] In essence, the various articles of the Directive mandate that:

---

the standards of the Directive in one form or another. For example, Germany and France have not adopted the Directive. *Id.* Nonetheless, discussions relating to the implementation of the Directive have occurred in their parliaments. In response, the European Court of Justice has taken legal action against various Member States for failing to implement the Directive within the established three year deadline. *Id.* These nations include Germany, Denmark, France, Ireland, Luxembourg and The Netherlands.

21. *See Data Protection, supra* note 11.

22. *See supra* note 1.

23. *Id.*

24. EUROPEAN COMMISSION, SUBMISSION TO THE HOUSE OF REPRESENTATIVES COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS CONCERNING ITS INQUIRY INTO THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000, at 4, *available at* http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf (last visited Feb. 23, 2002). This document also expresses the EU's fear that different approaches of the individual Member States would create barriers within the Single Market that would inhibit the free movement of personal data, thus threatening electronic commerce among EU Member States. *Id.*

25. Glenco McGraw-Hill, *The European Union Directive on Data Protection and You, at* http://www.glencoe.com/norton/n-instructor-/updates/1999/52699-7.html (last visited Feb. 23, 2002).

26. Council Directive 95/46, art. 3, 1995 O.J. (L 281) 31.

European companies who collect personal data from customers must:

(1) Post their privacy policies regarding the data.

(2) Specify the purpose for which the data is collected.

(3) Allow customers the right to review and correct data.

(4) Allow customers to opt out of data collection.

(5) Divulge which other organizations and companies may share the customer's data.

(6) Protect shared and transmitted customer data with adequate security.

(7) Limit customer data sharing to only those countries that have similar privacy laws.[27]

For Australia, the most important provisions of the Directive are Articles 25 and 26 because these concern the transfer of personal data to countries not part of the EU, or "third countries."[28] More specifically, Article 25(1) provides that Member States who transfer data to a third country may do so "only if, without prejudice to compliance with the national provisions adopted to the other provisions of this Directive, the third country in question ensures an adequate level of protection."[29] In addition, the European Commission ("Commission") has been given the power by the European Council and the European Parliament to determine on the basis of Article 25(6) whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.[30] Not only may a third country's do-

27. *Id.*

28. *Id.*

29. *Id.* art. 25(1).

30. *Id.* art. 25(6). As there is no case law on the issue, what constitutes an adequate level of protection has never been concretely established, or articulated by the EU. The only articulation to date is the standard promulgated in Article 25(2), which reads:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question

mestic law provide adequate protection, but the Commission has recognized that an adequate level of protection may be supplied by a sector specific legislative act or effective self-regulatory scheme, for example, one whose enforcement was underpinned by law.[31] As a result of the above provision, the Australian Parliament was forced to enact legislation providing an adequate level of protection to citizens of the EU so that Australian businesses could maintain commercial relations with EU businesses.[32]

III. AUSTRALIAN LEGISLATIVE HISTORY OF THE PRIVACY AMENDMENT

The result of Directive 95/46 in Australia and its stringent standards regarding the collection and transfer of personal data is the Privacy Amendment ("Private Sector") Bill 2000. In order to fully understand the Amendment, not only is the legislative history of the Directive important, but the history of the privacy concerns of the Australian populace, and the legislation that grew out of those concerns, must be examined as well.

In 1985, the Australian government addressed tax evasion, welfare fraud and illegal immigration when it introduced into legislation the Australia Card Bill ("Card Bill").[33] The Card Bill was supposed to be a nationally implemented means of multi-purpose identification.[34] If the legislation was ratified, each individual and organization was to be issued a card, a unique identification number and certain information reporting obliga-

---

and the professional rules and security measures which are complied with in that country.

Id. art. 25(2).

31. Council directive 95/46, *supra* note 26, art. 25(2).

32. However, one must not get the impression that Australia is a nation that has historically paid no attention to the privacy concerns of its citizens. For example, in 1984, Australia acceded to the OECD Guidelines. Roger Clarke, *A History of Privacy in Australia*, (Oct. 1998), *at* http://www.anu.edu.au/people/Roger.Clarke/DV/OzHistory.html [hereinafter *A History of Privacy*].

33. *Id.*

34. *Id.*

tions.[35] However, the Card Bill was defeated in the Senate by the combined efforts of the three non-Labor parties in December 1986 and March 1987.[36] In conjunction with the Card Bill, the Australian government tried to pass the Privacy Bill 1986; however, this Bill was tabled as it was attacked by privacy advocates as being completely inadequate.[37] In September 1987, the government withdrew the Card Bill and the Privacy Bill 1986 in response to a highly critical public.[38]

Although the Card Bill and Privacy Bill 1986 were never successfully ratified by the government, that did not cease future attempts. As an alternative to the highly criticized Card Bill, the Government "set out to significantly enhance the Tax File Number ["TFN"] scheme used by the Australian Tax Office."[39] To effectuate this goal, the government passed the Privacy Act.[40] The Privacy Act codifies the principles of the OECD Guidelines, and fulfills Australia's obligations under Article 17 of the International Covenant on Civil and Political Rights.[41] In addition, the Privacy Act establishes the Office of the Privacy Commissioner as a member of the Human Rights and

35. *Id.* For purposes of this commentary, it is unnecessary to delve into the specifics of the Card Bill, but the Bill is worth mentioning as an early attempt by the Australian government to allay privacy concerns and fears on a national scale.

36. *Id.*

37. *Id.*

38. *See A History of Privacy, supra* note 32. In his article, Roger Clarke states that "the Government used the opportunity afforded by the repeated rejection by the Senate of a Bill twice passed by the House of Representatives to call a double-dissolution election." *Id.* The matter was barely mentioned during the campaign, however. After the incumbent government won another term, the public outcry against both bills was so great it removed both bills from consideration. *See id.*

39. *Id.*

40. Office of the Federal Privacy Commissioner, *Background to the Privacy Act 1988*, *at* http://www.privacy.gov.au/act/index.html (last visited Feb. 23, 2002).

41. *Id.* Article 17 of the International Covenant on Civil and Political Rights states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has a right to the protection of the law against such interference or attacks." International Covenant on Civil and Political Rights, Mar. 23, 1976, art. 17, 999 U.N.T.S. 171, 177.

Equal Opportunity Commission.[42] For the most part, this Act applies to the public sector, but also regulates the private sector as well.[43] It applies to individuals in three ways: (1) the Act contains the Information Privacy Principles ("IPPs"), which regulate the collection, solicitation, alteration and security of personal data by the federal government and federal agencies;[44] (2) the Act prevents TFN's from being used as a national identification scheme by strictly limiting the use of TFN's to tax related purposes;[45] and (3) the Privacy Act strictly limits what the credit industry can do with the individual's credit information.[46]

Shortly after the government regulated the transfer of personal information in the public sector, concerns about private sector practices dramatically increased.[47] Great concern was expressed about the transfer of personal data by electronic means in areas such as debt collection, banking, insurance, direct marketing and telecommunications.[48] In 1995, a report published by the Australian Privacy Commissioner showed that an excess of 70% of Australians believed that computers reduced the level of privacy in Australia, and that almost 80% of Australian citizens felt that computers facilitated the means for unprivileged parties to gain access to confidential personal information.[49] Furthermore, only a small minority believed

42. *See Background to the Privacy Act 1988, supra* note 40. Currently, the Federal Privacy Commissioner is Malcolm Crompton. Office of the Federal Privacy Commissioner, *Privacy: About the Privacy Commissioner, at* http://www.privacy.gov.au/about/index.html (last visited Feb. 23, 2002). The purpose of the Federal Privacy Commissioner is "to promote an Australian culture that respects privacy." *Id.* Pursuant to the Privacy Act, the Privacy Commissioner is responsible for the protection of personal information handled by government agencies, personal tax file numbers used by individuals and organizations, and credit information. *Id.*

43. *See* INQUIRY I, *supra* note 2, at 6.

44. Privacy Act, 1988, pt. III (Austl.).

45. *Id.* pt. IX.

46. *Id.* pt. IIIA.

47. *See A History of Privacy, supra* note 32, at 4.

48. *Id.*

49. *See* INQUIRY I, *supra* note 2, at 6. For complete details and statistics of the survey and report, see Office of the Federal Privacy Commissioner, *Community Attitudes to Privacy, at* http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.word_file.p6_4_63.32.doc (last visited

there were adequate safeguards for personal information kept on computers, and only one in five were confident they understood how new technologies could affect their personal privacy.[50] The government took action in March 1997, when the Prime Minister and the Privacy Commissioner sought to develop a system of principles that would meet international privacy standards.[51] After numerous consultations with business and consumers, and the issuing of informational papers, the Privacy Commissioner issued the National Principles for the Fair Handling of Personal Information ("National Principles").[52] The National Principles were dubbed a flexible and relevant standard that businesses could follow without compromising the privacy interests of individuals.[53] On December 16, 1998, Australia announced it would regulate the protection of personal data in the private sector through the development of a "light touch legislative scheme."[54] This development, the Amendment, was introduced into to the Parliament on April 12, 2000.[55] The Amendment is supposed to supplement the Privacy Act, and became binding on December 21, 2001.[56] The Amendment regulates the acts and practices of business organizations, such as corporations.[57] It does this through the

---

d_file.p6_4_63.32.doc (last visited Feb. 23, 2002) [hereinafter *Community Attitudes to Privacy*].

50. *See Community Attitudes to Privacy, supra* note 49.

51. Office of the Federal Privacy Commissioner, *Privacy & the Private Sector*, *at* http://www.privacy.gov.au/private/index.html (last visited Feb. 23, 2002) [hereinafter *Privacy and the Private Sector*].

52. *See* NPPs, *supra* note 9.

53. *Id.* at 1.

54. *Privacy and the Private Sector, supra* note 50.

55. *See* INQUIRY I, *supra* note 2, at 6.

56. *See* Press Release, *supra* note 6. *See also* CAROLYN ADAMS ET AL., INFORMATION PAPER ON THE INTRODUCTION OF THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000 (2000), *at* http://law.gov.au/Privacy/ InformationPaper.html (last visited Feb. 23, 2002) [hereinafter INFORMATION PAPER].

57. The Amendment defines an organization as an individual, body corporate, partnership, or any other unincorporated association, or a trust "that is not a small business operator, a registered political party, an agency, a State or Territory authority or prescribed instrumentality of a State or Territory." Privacy Amendment (Private Sector) Bill, 2000, cl. 6C (Austl.).

implementation of the NPPs.[58] The purpose of the NPPs is to create a foundation upon which business organizations can develop commercial practices which ensure the protection of the individual's personal data.[59] In addition, the NPPs will bind all private sector organizations, unless they have an individual privacy code approved by the Privacy Commissioner.[60] Nonetheless, the NPPs offer some protection to private individuals. However, the protection they do offer is substantially undercut by the Amendment's small business exemption.[61] Thus, it remains to be seen whether the Amendment, once it becomes binding legislation, will live up to the stringent standards in Directive 95/46.

IV. COLLECTION OF PERSONAL INFORMATION

The collection of personal information is regulated by NPP Number One.[62] NPP 1.1 states that an organization is permitted to collect personal information that is necessary to carry on one or more of its functions or activities.[63] In almost all instances, for a corporation to do business over the Internet or through other electronic means, the collection of personal information will become necessary, especially since transactions over the Internet commonly require the submission of credit card information. Making the situation cloudier, the Amendment does not define the term collection. Therefore, collection is not necessarily limited to direct and obvious means. The only requirement is that an organization not collect personal

58. *Id.* The NPPs are the embodiment of the National Principles in legislative form. As the National Principles are merely guidelines that businesses were encouraged to adopt, they are the binding embodiment of the National Principles.

59. *Id.* The purpose of various NPPs, their relation to e-commerce and whether these principles accomplish their goal will be discussed at greater length in the sections to come.

60. *See* INFORMATION PAPER, *supra* note 56, at 3. The text of this submission goes on to state that, when the Privacy Commissioner takes into account whether a business organization should be given a privacy code, he must consult pt. IIIAA, cls. 18BA-18BG of the Amendment.

61. *See* INQUIRY I, *supra* note 2, at 7.

62. Amendment Bill, ¶ 139, NPP 1.

63. *Id.*

information in ways that are unlawful, unfair and unreasonably intrusive.[64] These standards are very general, and may be easily taken advantage of by organizations. As mentioned above, the use of cookies and Web Bugs is perfectly legal in Australia, and Parliament has not indicated that it plans to curtail such deceptive practices. Thus, if information collection by invisible computer programs is acceptable, then what form of direct collection would be considered unreasonably intrusive? Furthermore, NPP 1.2 does not say whether the indirect gathering of personal information constitutes collection. Thus, is personal information "collected if it is indirectly derived by correlation from other data held by that organization or another organization?"[65]

In addition, corporations would not have a hard time staying within the realm of practices permitted by NPP 1.2 as it is controlled by a reasonableness standard.[66] It is possible that two major corporations, The Walt Disney Company ("Disney") and Amazon.com, Inc. ("Amazon.com"), may make such an argument.[67] As of May 7, 2000, the privacy policy available to Dis-

---

64. *Id.*

65. AUSTRALIAN CONSUMERS' ASS'N TO HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS, INQUIRY INTO PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000 (2000), *at* http://www.aph.gov.au/house/committee/laca/Privacybill/sub30.pdf (last visited Feb. 23, 2002) [hereinafter ACA]. This submission asks a variety of questions that remain unanswerable because Parliament neglected to define "collection." For instance, it is unclear whether personal data that is updated or corrected is considered collected. *See id.* at 4. If the answer to this question is no, then an organization can use updated or corrected personal information for any purpose because non-collected data does not fall within the guise of the Amendment. Hypothetically, a problem like this could arise when an individual receives a new credit card that has a new account number and expiration date. Thus, when the individual submits the new account number to the organization, that personal data may not be considered "collected."

66. *See* Amendment Bill, ¶ 139, NPP 1. The text of NPP 1.2 reads "[a]n organization must collect personal information only by lawful and fair means and not in an unreasonably intrusive way." *Id.* at NPP 1.2.

67. The privacy policies promulgated at Disney.com and Amazon.com will be used as examples of how extremely verbose and complex policies fall within the legal confines of the Amendment.

ney's website contained 2,242 words.[68] Also, the privacy policy at Amazon.com's website contains over 1,000 words.[69] Although Amazon.com's policy is less than Disney's, the fact that both policies are so lengthy may discourage the average individual from reading the entire statement. However, significant negative consequences may arise for the consumer unwilling to spend valuable time reading these wordy policies. For example, the privacy policy on the Disney website states, "[b]y using this site, you signify your assent to the Disney Online and the Go Network Privacy Policy."[70] Thus, by merely clicking on Disney's website one is subject to the personal information collection practices of Disney and the Go Network promulgated in the privacy policy. It is highly likely that this collection practice will be legal under the reasonableness standard set forth by the Amendment in NPP 1.2. This practice is valid under NPP 1.2 because all the clause requires is collection in a lawful, fair and not unreasonably intrusive manner.[71] The collection of personal information is lawful because the Amendment does not proscribe this practice. It can be argued that personal information collection in this manner is fair and not unreasonably intrusive because data is collected through the use of cookies.[72] As stated above, cookies are a legal and common method of data collection on the Internet.[73] Furthermore, it would be extremely impractical for an Australian judge hearing this case of first impression to hold that the use of cookies is forbidden in

68. THE COALITION AGAINST UNSOLICITED BULK EMAIL, AUSTRALIA (CAUBE.AU), SUBMISSION FOR INQUIRY INTO THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000, at 8 (2000), *available at* http://www.aph.gov.au/house/committee/laca/ Privacybill/sub39.pdf (last visited Feb. 23, 2002) [hereinafter CAUBE.AU]. For further information on CAUBE.AU, see http://www.caube.org.au.

69. *Id.* at 8. However, Amazon.com recently revised their privacy policy. D. Ian Hopper, *Consumer Groups Criticize Amazon's New Privacy Policy*, NEWS, Sept. 2, 2000, at D1. For the new version, see http://www.Amazon.com.

70. *See* CAUBE.AU, *supra* note 68, at 8 (stating that the CAUBE.AU submission has attached as appendices the entire privacy policies of Disney and Amazon.com).

71. *See* Amendment Bill, ¶ 139, NPP 1.2.

72. *See* CAUBE.AU, *supra* note 68, at 12.

73. *See* INQUIRY I, *supra* note 2, at 3.

Australia. It would be impractical because of the apparent global acceptance of cookies as an electronic phenomenon. In addition, it would be an unenforceable and economically unwise decision. Certainly, Disney and Amazon.com would not stop using cookies solely because an Australian judge ordered them to. Thus, the only way to prevent the use of cookies in Australia would be to prevent the Australian populous from going online, and this will never happen.

Once personal data is collected by an organization, that organization is statutorily obligated by NPP 1.3 to reasonably ensure that the individual is aware of certain things.[74] Once again, the problem with this clause is the use of the phrase "reasonable steps."[75] Thus, the Amendment creates a standard that many corporations can satisfy, even with extremely lengthy privacy policies. For example, NPP 1.3(c) requires a business organization to take reasonable steps to tell the individual the purposes for which the information is collected.[76] Again, Disney and Amazon.com can be used as examples of businesses that may successfully argue they acted reasonably when they located the purposes for which the personal data was going to be used in a 1,000 line privacy policy.[77] Disney's policy states the purposes and possible uses of a customer's or Internet surfer's personal data.[78] The actual text of the policy reads:

> Information provided at the time of Registration or submission from a Guest who is 13 years of age or over may be used

---

74. NPP 1.3 lists six reasonable steps:

> (a) the identity of the organization and how to contact it; and (b) the fact that he or she is able to gain access to the information; and (c) the purposes for which the information is collected; and (d) the organizations (or types of organizations) to which the organization usually discloses information of that kind; and (e) any law that requires the particular information to be collected; and (f) the main consequences (if any) for the individual if all or part of the information is not provided.

Amendment Bill, ¶ 139, NPP 1.3.

75. *Id.* at NPP 1.3.

76. *Id.*

77. *See* CAUBE.AU, *supra* note 68, at 7.

78. *Id.* at 7.

> for marketing and promotional purposes by Disney Online, the Go Network, and our affiliates or companies that have been prescreened by Disney Online and the Go Network.[79]

Unless a visitor to the Disney website reads the entire 2,200 word document, he or she is unwittingly subjecting themselves to the appropriation of their personal data for commercial uses, not only by Disney, but also by Disney's affiliates, other members of the Go Network and any other companies "prescreened by Disney or the Go Network."[80] By enacting a reasonableness standard, the Amendment magnificently succeeds in fostering the interests of electronic commerce, while simultaneously subordinating individual privacy. A court would likely find that Disney took reasonable steps to ensure the individual is aware that his or her personal data will be used for direct marketing or promotional purposes.

Similar to Disney, Amazon.com states that they will use personal data for marketing purposes.[81] Amazon.com goes further than Disney by reserving the right to "share their customer's personal data to third parties."[82] Even though it may appear

---

79. *Id* at 11. *See also* Disney.com, *Privacy Policy*, at http://disney.go.com/legal/privacy_policy.html. In addition, to prevent the direct marketing and promotional use of the individual's personal data, they must affirmatively request Disney to stop. *Id.* The text of the policy states: "If a Guest objects to such use for any reason, he/she may stop that use - either by e-mail request to guest.mailonline.disney.com or by modifying his/her member information online." *Id.* The affirmative request by an individual to an organization to stop the use of their personal data is called "opting out." An in depth discussion of the opt out policies and the problems they present will be addressed later.

80. *See* CAUBE.AU, *supra* note 68, at 11 (in addition, the privacy policy does not specify the methods of "prescreening").

81. *See* Hopper, *supra* note 69. The pertinent language in the privacy policies is as follows: "To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer supports such capabilities. We also compare our customer list to lists received from other companies, in an effort to avoid sending unnecessary messages to our customers." Amazon.com, Inc., *Privacy Policy, at* http://www.Amazon.com (last visited Feb. 23, 2002) [hereinafter *Privacy Policy*]. Thus, Amazon.com admits they send e-mails based on personal information they collect and information collected from third parties.

82. *Privacy Policy*, *supra* note 81. The pertinent paragraph in Amazon.com's privacy policy is as follows: "Information about our customers is an

that the practice of selling someone's personal data to a third party may seem unethical, the Amendment does not prohibit it.[83] NPP 1.3(a) merely requires that the organization take reasonable steps to make the individual aware of the organization's identity and how to contact it.[84] Amazon.com's privacy policy satisfies this provision, as the organization's identity is obvious, and the privacy policy discloses an e-mail address that can be used to contact the organization.[85] The requirement of NPP 1.3(b) is satisfied as the Amazon.com policy allows customers to gain access to their information to update or change it.[86] Furthermore, Amazon.com's privacy policy is legal pursuant to NPP 1.3(c) because the policy clearly manifests its intent to share its customers' information with subsidiaries that Amazon.com controls.[87] It can be argued that NPP 1.3(d) is also met, because a court would likely hold that Amazon.com acted reasonably by stating that personal information is only shared with its subsidiaries, presumably trustworthy organizations.[88] Arguably, the Amendment's reasonableness standard requires

---

important part of our business, and we are not in the business of selling it to others. We share customer information only with the subsidiaries Amazon.com, Inc., controls and as described below." *Id.* Although Amazon.com claims they do not sell their customer's personal information, this statement is extremely misleading. For example, the policy states:

> As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets. Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Id. Thus, Amazon.com will sell the customer information it collects, and this attempt to hide such information may not be detected by the casual consumer, and it will not be detected by the average individual who does not endeavor to read such lengthy and misleading documents. However, such practices are legal pursuant to the Amendment.

83. *See generally* Amendment Bill, ¶ 139, NPP 1.3(a).

84. *Id.* ¶ 139, NPP 1.3(a).

85. *See Privacy Policy, supra* note 81.

86. *Id.*; *see also* Amendment Bill, ¶ 139, NPP 1.3.

87. *See Privacy Policy, supra* note 81; *see also* Amendment Bill, ¶ 139, NPP 1.3.

88. *See Privacy Policy, supra* note 81; *see also* Amendment Bill, ¶ 139, NPP 1.3.

nothing more than this. The Amendment does not require the organization that collects personal data to specifically state the organizations with whom they share information, and the criteria regulating disclosure of information to third parties does not appear to restrain Amazon.com from engaging in this practice.[89] Finally, Amazon.com's privacy policy satisfies NPP 1.3(f).[90] If the individual does not provide certain information, then some features of the Amazon.com website will not function properly.[91] Thus, even though Amazon.com reserves the right to collect and sell the personal data of the unwitting consumer, this practice is legal under the Amendment's reasonableness standard.

Through the use of a reasonableness standard, it can be argued that NPP 1.3 conflicts with the purposes of the Amend-

89. *See generally* Amendment Bill. In addition, the provision controlling organizations that disclose personal information to third parties is NPP 2.1(c). *Id.* ¶ 139, NPP 2.1(c). NPP 2.1(c), which will be discussed in greater depth *infra,* reads as follows:

> An organization must not use or disclose personal information about an individual for a purpose (the *secondary purpose*) other than the primary purpose of collection unless . . . the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
>
> (i) it is impracticable for the organization to seek the individuals consent before that particular use; and
>
> (ii) the organization will not charge the individual for giving effect to a request by the individual to the organization not to receive direct marketing communications; and
>
> (iii) the individual has not made a request to the organization not to receive direct marketing communications; and
>
> (iv) the organization gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications . . . .

Id. The privacy policy of Amazon.com states that personal data will be used for direct marketing purposes, and as discussed *infra,* the practices of Amazon.com fall within the legal realm of the Amendment. *See Privacy Policy, supra* note 81.

90. *See* Amendment Bill, ¶ 139, NPP 1.3. In addition, NPP 1.3(e) does not really apply because it only mandates that organizations make individuals aware of any law requiring the collection of information. *Id.* In any event, this provision could be satisfied by merely placing in the middle of large policy the pertinent law.

91. *See Privacy Policy, supra* note 81.

ment. One of the main objectives stated in the Amendment is the recognition of privacy as an important right that necessitates protection through the enactment of a comprehensive national privacy plan.[92] In actuality, the Amendment does not truly protect privacy interests because it allows an organization to bury its intent deep within its privacy policy. Furthermore, the Amendment does not require websites to even have privacy policies.[93] It merely requires collection of personal data through reasonable means, and once data is collected, that the individual is reasonably made aware of the purposes for which the data will be used.[94] The Amendment is not supplemented by any legislative history or examples of what is considered reasonable.[95] Thus, the Australian judicial system will have no legislative guidance when deciding what is reasonable. Third, the reasonableness standard places Australian judges in an extremely precarious, if not impossible, role because they must weigh the reasonable acts and commercial interests of multinational corporations against the privacy rights of the individual.[96] Once a decision is made, many enforcement issues will arise.[97]

V. DIRECT MARKETING & OPTING OUT VERSUS OPTING IN

NPP 2.1 regulates the use and disclosure of personal information.[98] However, NPP 2.1 regulates the use and disclosure of

92. Amendment Bill, pmbl., ¶ 3.

93. *See generally id.*

94. *See id.*

95. *See id.*

96. In addition, the corporations will not always be Australian corporations and problems of jurisdiction over these corporations may arise. For example, does a court have jurisdiction over a corporation who merely makes its website available to foreign nationals? It can be argued that there is no jurisdiction because the corporation did not act affirmatively in Australia. Rather, it was an Australian citizen who logged onto the non-Australian corporation's website, simply looked around, bought nothing, and then left.

97. Enforcement of judicial decisions by Australian Courts over the business practices of non-Australian corporations is not the focus of this discussion. It is only important to state the possibility of their existence.

98. *See generally* Amendment Bill, ¶ 139, NPP 2.1. In addition, NPP 2.1 does not cover the use and disclosure of personal information for the purpose for which the information was collected, or the "primary purpose." MALCOLM

personal information for a "secondary purpose."[99] Specifically, the Amendment regulates the use of personal information for the secondary purpose of direct marketing in NPP 2.1(c).[100] Marketing is the communication, by a marketer, concerning the sale of goods or services to prospective customers.[101] The communications proffered from the marketer to a prospective customer can provide information regarding features, conditions of purchase, availability and image, and as such, are intended as direct stimuli to a purchasing decision.[102] In other words, the ideal marketer will bombard the average individual with as much information as possible in an attempt to ensure an informed consumer decision. Two of the basic categories of marketing are indirect and direct.[103] A communication from a marketer to a customer is indirect when interactions between the marketer and the prospective customer are inhibited.[104] There are several reasons why these communications may be inhibited.[105] For example, there may be only a one-way path of communicable information, as in the use of broadcasting media like television, radio, newspapers and billboards.[106] In addition, communications may be indirect because an intermediary that does not have a principal-agent relationship with the marketer may be in between the marketer and the prospective customer.[107]

CROMPTON, PRIVACY COMMISSIONER'S REPORT ON THE APPLICATION OF THE NATIONAL PRINCIPLES FOR THE FAIR HANDLING OF PERSONAL INFORMATION TO PERSONAL HEALTH INFORMATION 20 (2000), *available at* http://search.aph.gov.au/search/ (last visited Feb. 23, 2002).

99. *See generally* Amendment Bill.

100. *Id.* ¶ 139, NPP 2.1(c).

101. Roger Clarke, *Direct Marketing and Privacy*, (Feb. 23, 1998), *at* http://www.anu.edu.au/people/Roger.Clarke/DV/Directmkting.html [hereinafter *Direct Marketing*].

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

107. *See Direct Marketing, supra* note 101. For example, a shop assistant in a retail department store. *See id.*

A second type of marketing is direct marketing.[108] The characteristics of direct marketing are direct communications between the marketer and prospective customer without the existence of an intermediary, and the channel of information allows interaction between the marketer and the prospective customer.[109] One of the primary features of direct marketing is the emphasis on data collection of individuals, and the subsequent storage of this information in databases.[110] Marketers prefer to utilize methods of direct marketing because it has the advantages of "cost reductions, arising from the nature of the channels and the automation of communications, extended reach, arising from the nature of the channels[,] and enhanced conversion-rates from prospect to purchaser, as a result of customized targeting based on data about each prospect."[111]

The most important feature of direct marketing pursuant to the Amendment, and more specifically NPP 2.1(c)(iii), is that Australian citizens are not protected from having the costs of direct marketing placed upon them.[112] In terms of costs, there are two categories of direct marketing.[113] The first type is marketing that costs the individual nothing, such as mailings or

---

108. *Id.*

109. *Id.* In addition, the physical range, in terms of proximity, of contact made available by direct marketing can be divided into two groups: direct marketing that involves close physical proximity between the marketer, or an agent of the marketer and prospective customers. *See id.* This includes marketing on the marketer's own premises, or at the prospective customer's home. *See id.* Direct marketing through electronic means is known as "direct marketing at a distance." *Direct Marketing, supra* note 101. Direct marketing in this fashion endeavors to communicate with a greater proportion of the target population than direct marketing at proximity. *See id.* Furthermore, direct marketing at a distance seeks to communicate with prospective customers "with an immediacy and apparent relevance that motivates purchase, and to do so for relatively low cost." *Id.*

110. *Id.*

111. *Id.*

112. *See* Amendment Bill, ¶ 139, NPP 2.1(c).

113. NAT'L PARTY COMMUNICATIONS & INFO. TECH. POLICY COMM., SUBMISSION TO HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS REGARDING THE INQUIRY INTO PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000, at 6 (2000), *at* http://www.aph.gov.au/house/committee/laca/Privacybill/sub36.pdf (last visited Feb. 23, 2002) [hereinafter NAT'L PARTY].

telemarketing.[114] Alternatively, methods of direct marketing, such as e-mail, costs the individual money to receive the information.[115] One common form of this direct marketing is spam.[116] Spam is unsolicited communication through electronic media.[117] The Amendment permits business organizations to send spam to prospective consumers so long as the information is being sent for direct marketing purposes.[118] In addition, it is the responsibility of the individual to make a request that the organization stop sending them such communications in the future.[119] Placing the burden on the individual to affirmatively request that the organization cease sending marketing communications is known as "opting out."[120] The consequences of the opt out provision will be monumental. Thus, the Australian government is communicating to marketers that it is legal to pass advertising costs on to *all* Australians, and even residents of other countries, whether they are customers or not and whether they want to receive advice regarding your products or services or not. This is an entirely new concept at law.[121]

The problem with NPP 2.1(c)(iii), therefore, is that it allows direct marketers to advertise their products and services to the detriment of those who are not even their customers. In addition, why should an individual be charged for the receipt of an unwanted solicitation before he or she even knows that the e-

---

114. *Id.*

115. *Id.* at 4. The reason that spam costs the recipient money is because it costs Internet service providers ("ISPs") money, who then pass on these costs to their subscribers. *See id.* Thus, spam makes using the Internet more expensive for everyone, except the marketers. *See id.* Also, spam places costs on Internet usage because there are limitations on the amount of disruptions that an ISP can handle before it crashes, and ISPs spend millions of dollars per year correcting crashes. *Id.*

116. NAT'L PARTY, *supra* note 113, at 4.

117. *See Direct Marketing*, *supra* note 101. Mr. Clarke points out that spam is conducted by mailing to an e-list, or by posting to an electronic forum such as a newsgroup, web or IRC-based e-chat session. *Id.*

118. *See generally* Amendment Bill, ¶ 139, NPP 2.1(c).

119. *See id.*

120. NAT'L PARTY, *supra* note 113, at 6. (as opposed to opting in where the organization would not send solicitations and other information to individuals unless an individual requested that the organization do so).

121. *See id.*

mail is such a solicitation?[122] Further, it is not unusual for an individual to receive in excess of ten pieces of spam per day.[123] Compounding this problem is the fact that direct marketing is growing at an almost exponential rate.[124]

The problem is that the Amendment allows unsolicited and unwanted e-mails that cost virtually nothing to be sent, and cumulatively can be very expensive to the recipient.[125] As direct marketing through electronic media rapidly increases in the near future, this may mean that traditional forms of direct marketing that cost the marketer money, such as telemarketing and mailings may become extinct, thereby increasing the costs to the average individual.[126]

---

122. *Id.* For example, this submission tells such a story of a woman in Australia who was the recipient of a two megabyte e-mail over a standard phone line. The e-mail cost the woman fifty Australian cents merely to receive the unsolicited e-mail, in addition to the phone charges for the hour it took to download the e-mail. *Id.* In sum, the woman was charged two Australian dollars for an advertisement she did not want. *Id.* However, the text of the submission goes on to state that this is an extreme example, and that the average spam costs approximately four Australian cents to receive, plus phone charges for downloading time, and standard ISP downloading charges of twenty Australian cents per megabyte. *Id.* In addition to e-mails, faxes are also considered a mode of electronic communication, and cost paper, ink and electricity to be received. NAT'L PARTY, *supra* note 113, at 6.

123. *Id.* at 7. Furthermore, it cost Pacific Bell approximately $500,000 in repairs because three pieces of spam were sent simultaneously. *Id.* at 23. The "I Love You" virus costs billions of dollars in repairs which will be passed onto the consumer from the ISP. *Id.*

124. *See* AUSTL. DIRECT MARKETING ASS'N, SUBMISSION TO THE HOUSE OF REPRESENTATIVES COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS CONCERNING ITS INQUIRY INTO THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000 (2000), *at* http://www.aph.gov.au/house/committee/laca/Privacybill/sub44.pdf (last visited Feb. 23, 2002). The text of this submission states that direct marketing is now half of all media spending at over nine billion dollars a year spent on advertising media, and that direct marketing is growing at 15% a year. *Id.* at 5. This means that by the year 2001, direct marketers will spend $210 million on Internet advertising. *Id.*

125. *See* CAUBE.AU, *supra* note 68, at 2.

126. *See* NAT'L PARTY, *supra* note 113, at 7. For example, in order for an organization to send a communication via traditional mail, it must pay the postage before sending the letter, or a phone call cannot be made unless the caller pays a fee beforehand. *Id.* Even in the case of a collect call, the recipient is given the option of accepting the call, and is told who is making the call. *Id.*

In addition to economic costs to the consumer, the lax standard of the Amendment in relation to direct marketing and spam may create significant economic costs to the marketer.[127] Numerous studies, such as the *Pulse of the Consumer,* that "dealt primarily with unexpected marketing intrusions from companies that the recipient had actually dealt with previously concluded that consumers dislike receiving spam."[128] It is ironic that the very practice that marketers use to attract customers in fact causes them to lose prospective business.[129]

Fundamentally, a consumer must have confidence in the economy, especially the electronic economy, as electronic commerce via the Internet appears to be the wave of the future.[130] The personal data of an individual should not be the measure of the individual. In other words, electronic commerce will continue to prosper only if individuals are treated as such by organizations. Thus, they must not be dehumanized and their personal data viewed objectively as mere assets for sale in the open market.[131] Since the relaxed standards of the Amendment would allow personal information to be treated as an asset, the

---

127. *See* CAUBE.AU, *supra* note 68, at 2.

128. *Id.* The *Pulse of the Consumer* study stated that "[o]ne-third of all respondents say they dislike sales-oriented email so much that it actually makes them avoid the vendor who sends them." *Id.* The numerous studies revealed that between 33% and 65% are adverse to receiving spam. *Id.* at 3.

129. The government acknowledged the benefits of e-commerce, and the problems of spam direct marketing when it stated:

> Many potential misuses can impose a direct cost on the consumer. Spam email and direct marketing via bulk facsimile transmission are examples. If the transfer of an individuals email address or fax number (along with other information such as purchasing habits) results in that person receiving unsolicited communications, the nature of email and fax as a form of communication means that the cost of delivery will be largely born by the recipient. This is also the case with consumers cost in contacting the organization to request no further communications.

Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000, at 26 (2000).

130. Privacy Commissioner Malcolm Crompton has even stated: "Ultimately, the future of e-commerce will be based on trust and consumer confidence. When your competitor is only a 'mouse-click away', trust will be a strong competitive advantage." *See* CAUBE.AU, *supra* note 68, at 3.

131. *See* Hopper, *supra* note 69.

objective of protecting the individuals' privacy interest is not fulfilled.[132] Admittedly, one of the "objects in the Amendment is the economic efficiency of businesses."[133] Nevertheless, economic efficiency should not come at the expense of the individual's right to protect one's own information from being used by organizations to make a profit.[134] Thus, it is fair to state that the privacy rights enumerated in the Amendment are nothing more than an attempt of Parliament to foster Australia's international economy via the Internet, while at the same time acting as a pretext to placate the privacy concerns of Australians.

VI. THE SMALL BUSINESS OPERATOR EXEMPTION

One of the most innovative, yet problematic provisions in the Amendment is the "small business exemption."[135] This exemp-

---

132. The third introductory section of the Amendment, titled "Objects," states:

> The main objects of this Act are:
>
> (a) to establish a single comprehensive national scheme providing, through codes adopted by private sector organizations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organizations; and
>
> (b) to do so in a way that:
>
> (i) meets international concerns and Australia's international obligations relating to privacy; and
>
> (ii) recognizes individuals interests in protecting their privacy; and
>
> (iii) recognizes important human rights and social interests that compete with privacy, including the general desirability of a free flow information (through the media and otherwise) and the right of business to achieve its objectives efficiently.

Amendment Bill, pmbl., ¶ 3.

133. *Id.*

134. However, this is exactly what the conflicting provisions of the Amendment's "Objects" section and the ability of organizations to use personal information for direct marketing purposes allow.

135. "A business is a *small business* if its annual turnover is $3,000,000 or less." Amendment Bill, ¶ 36, 6D. The annual turnover of a small business is determined by measuring the current annual income of a business at a specified test time in a test month pursuant to "subsection 188-15(1) of the *A New Tax System (Goods and Services Tax) Act 1999*," and meets additional qualifi-

tion applies to economic enterprises making less than $3,000,000 per year.[136] In short, economic enterprises with an annual turnover less than $3,000,000 are removed from the definition of "organization" and are placed in the category of "small business operator," thus exempting them the Amendment's application.[137] Further, the small business exemption prescribes the application of the Amendment to small business operators for twelve months after the Amendment becomes binding.[138] The twelve month period is an adjustment period to give the small business operators an opportunity to conform with the Amendment.[139] Once the twelve month grace period is over, all businesses that qualify as small business operators will continue to be exempt from the legislation unless they: (1) carry on a business with an annual turnover in excess of $3,000,000 at any time after the later of the commencement of the business, or the commencement of this section of the Amendment;[140] (2) provide health services to another individual and hold health information, except in an employee record;[141] (3) discloses personal information about another individual to anyone else for a benefit, service, or advantage;[142] (4) provide a benefit, service, or advantage for the collection of personal information about anyone else from anyone else;[143] (5) provide a

---

cations not pertinent to this discussion. *Id.* However, the use of the phrase "small business" is confusing because the exemption really applies to commercial entities known as "small business operators." *Id.*

136. Pursuant to the Amendment, an organization is defined as (a) an individual; or (b) a body corporate; or (c) a partnership; or (d) any other incorporated association; or (e) a trust; that is *not a small business operator*, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory. Amendment Bill, ¶ 36, 6C (emphasis added).

137. *Id.* They are exempt because the Amendment applies only to organizations.

138. Office of the Federal Privacy Commission, *Fact Sheet: Privacy, Small Business and Employee Records*, (Apr. 12, 2000), *at* http://www.law.gov.au/privacy/empfact.html (last visited Feb. 23, 2002).

139. *Id.*

140. Amendment Bill, ¶ 36, 6D(4)(a).

141. *Id.* at 6D(4)(b).

142. *Id.* at 6D(4)(c).

143. *Id.* at 6D(4)(d).

contracted service to the Commonwealth;[144] or (6) the statute otherwise removes them from coverage of the small business exemption.[145]

In addition, the Attorney General can consult with the Federal Privacy Commissioner, and if they decide it is within the public's best interests, they have the authority to place within the ambit of the Amendment certain acts, otherwise exempted, which may constitute an extraordinary threat to the individual's privacy.[146] The complex structure of the exemption, created by the use of the Australian tax laws as the means by which organizations qualify as a small business, creates problems for the average consumer who is expected to decide whether an organization is required to satisfy the privacy standards.[147]

The small business exemption is problematic in several regards. Many Australian businesses will fall within the scope of the exemption, and thus have no obligation to maintain the privacy standards set forth in the Amendment.[148] In addition, many Internet service providers and other organizations that transfer personal information over the Internet have annual turnovers less than $3,000,000.[149] Thus, a great number of organizations in Australia, such as direct marketers, will qualify

144. *Id.* at 6D(4)(e).

145. Amendment Bill, ¶ 36, 6C.

146. *Id.*

147. AUSTL. PRIVACY CHARTER COUNCIL, PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000: INQUIRY BY THE HOUSE OF REPRESENTATIVES COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS 5 (2000), *at* http://www.aph.gov.au/house/committee/laca/Privacybill/sub57.pdf (last visited Feb. 23, 2002) [hereinafter PRIVACY CHARTER]. *See also* ACA, *supra* note 65, at 5 (the Australian Consumers' Association recommends that the small business exemption be completely removed from the Amendment). The ACA states that the individual's privacy would be more efficiently protected if the burden was placed on organizations to respect personal property, instead of leaving the difficult responsibility of judging which organizations are covered by the exemption to the consumer. *Id.*

148. GRAHAM GREENLEAF, SUBMISSION TO THE HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000, at 5 (2000), *at* http://www.aph.gov.au/house/committee/laca/Privacybill/sub64.pdf (last visited Feb. 23, 2002) [hereinafter GREENLEAF].

149. *See* INQUIRY II, *supra* note 12, at 7.

as "small business operators" and have no obligation to protect the privacy concerns of anyone.[150] Nevertheless, if a direct marketer has an annual turnover in excess of $3,000,000, nothing in the Amendment prohibits the direct marketer from reorganizing its structure into several smaller sibling businesses each of which make less than $3,000,000, and consequentially fall within the exemption.[151] The ramifications of such an act would be extremely far reaching because the individual businesses, in addition to falling within the exemption, would be free from any regulation of the transfer of personal information among them.[152] Since corporations, partnerships, and other business enterprises that carry on one or more small businesses, each of which turnover less than $3,000,000, are defined within the Amendment as a single "small business operator," there would be no transfer of personal information, and no applicable regulation.[153] Presumably, each of the sibling businesses would disclose personal information to each other free of cost, thus remaining within the guise of the exemption.[154] In addition, section 6D(4) regulates only the "disclosure of personal information," and not the "use of information."[155] Thus, the sibling business can use the information they receive from the other siblings for any purpose they wish and remain within the exemption.[156] However, the most disturbing revelation created by this scenario is that the individuals whose personal

150. However, not all businesses that fall within the exemption will be absolutely exempt. *See* Amendment Bill, ¶ 36, 6D(4)(b). For example, small businesses that collect and handle health and other sensitive information, the misuse of which has a greater potential for violations of the individual's privacy are not exempt. *See* CAUBE.AU, *supra* note 68, at 6.

151. *See* PRIVACY CHARTER, *supra* note 147, at 5.

152. *Id.*

153. Amendment Bill, ¶ 36, 6D(3). PRIVACY CHARTER, *supra* note 147, at 5.

154. *See* Amendment Bill, ¶ 36, 6D(4)(c). In order for the sibling businesses to be removed from the exemption they would have to disclose their personal information to other siblings for a benefit, service, or advantage. *Id.* However, sibling corporations would never engage in such actions, as they would impose costs, thereby hindering business efficiency. *Id.*

155. *Id.* at 6D(4).

156. *See* GREENLEAF, *supra* note 148, at 6. This proposition is true, "even if the use is completely unrelated to the purpose of collection, and if the information used is inaccurate, irrelevant, incomplete etc." *Id.*

information is collected and used for any purpose, without that information being disclosed, have no way to prevent this, and no means of legal redress.[157]

In addition to the problems the small business exemption poses to the privacy rights of individuals, it also creates problems for other small businesses. The small business exemption increases the value of sibling businesses with a wealth of personal information that can legally be shared between those enterprises without fear of regulation.[158] The value of a small business operator with personal information is increased because other businesses will prefer to purchase a business with more information than not.[159] It could also be argued that the small business exemption will encourage small business operators to sell their entire enterprise, and not merely their information, thus encouraging tender offers and corporate takeovers. If a small business operator sells its information it will lose its exempt status because it would have disclosed personal information about an individual to anyone for a benefit, service or advantage.[160] Conversely, small business operators will be encouraged to purchase other small business operators, and not merely their information, because simply purchasing the personal information would remove the purchaser from the protection of the exemption.[161] In addition, once the target small

157. *Id.* ("Just have lots of 'small' privacy invading businesses, and your total business operation can be as big as you like, and still remain a privacy-free zone.").

158. Amendment Bill, ¶ 36, 6D(4).

159. It is logical that a small business operator would want to buy another small business operator with a wealth of personal information, thereby receiving access to its information, as opposed to solely buying that small business operator's information. *See* GREENLEAF, *supra* note 148, at 7. Furthermore, the purchasing small business operator would greatly benefit since it will gain the assets, employees, earnings, good will and other intangibles of the target small business in addition to its personal information.

160. *See* Amendment Bill, ¶ 36, 6D(4)(c).

161. *See id.* at 6D(4)(d). A possible indirect consequence of the small business exemption is an increase in hostile tender offers. There are several well known arguments against hostile tender offers. For example, opponents argue that hostile tender offers are harmful to non-shareholder constituents of a corporation, such as its employees and creditors because the purchasing corporation may sell the target corporation's assets, or fire the newly ac-

business operator is purchased, the purchaser can freely share that information with its new siblings free of regulation.[162] Thus, businesses that restructure their organization to fall within the small business exemption will have a higher value than businesses that do not. Consequently, personal information is once again treated as an asset for sale in the market, thereby undermining the stated privacy objective of the Amendment.[163]

VII. TECHNOLOGICAL SOLUTIONS

Consumers and potential consumers via the Internet are obviously concerned about how businesses will use their personal information.[164] However, statutory regulation by itself will not

---

quired employees. ARTHUR R. PINTO & DOUGLAS M. BRANSON, UNDERSTANDING CORPORATE LAW 307 (1999).

It can also be argued that hostile tender offers destroy technological creativity because corporate executives and officials would rather focus on how to take over another corporation with valuable assets, as opposed to problem solving within their own enterprise by creating new technologies which would enhance the market through competition. In terms of the use of personal information for commerce and direct marketing via the Internet, the consequences on privacy could be extremely detrimental to the individual. For instance, the loophole in the small business exemption encourages organizational restructuring of businesses, which could lead to increased sales of corporations for their personal information, thereby discouraging the advent of technologies to protect personal information. This begs the question why would a small business operator with enough capital to purchase another small business operator with valuable personal information want to create technologies that protect personal information, as opposed to profiting off the unregulated use of the purchasable information? Another possible consequence of this scenario is a bidding war between businesses over a small business operator with valuable personal information. Thus, the loophole in the small business exemption inadvertently turns personal information into a marketable asset.

162. *See* Amendment Bill, ¶ 36, 6D(3).

163. *See id.* pmbl.,¶ 3.

164. In 1999, Privacy & American Business conducted a survey which "found that a staggering 92 percent of consumers are concerned about the potential misuse of their personal data online." Edward Robinson, *Click and Cover*, BUSINESS 2.0 (Aug. 22, 2000), *at* http://www.business2.com/content/magazine/indepth/2000/08/22/17281. Although this study was conducted in the United States, it is hard to see why results would greatly differ in Australia. In addition, the protection of personal information collected online is a problem that transcends national borders, especially in an increasingly global

suffice, as clever businesses will find loopholes in statutory schemes.[165] Thus, software designers are attempting to solve these concerns in the form of marketable software programs for use in the private sector.[166] Such software programs have been dubbed privacy enhancing technologies ("PETs").[167] It is important to keep in mind that PETs are not solutions in themselves, but should be used in conjunction with stringent statutory standards, as well as an affirmative attempt of businesses themselves to meet the concerns of their consumer.[168]

The first of these technological techniques are digital signatures. They will be used as a means of encoding sensitive information sent over the Internet, such as credit card information.[169] Digital signatures are long numbers associated with a specific individual that are used to guarantee that information or a message belongs to that individual.[170] As they are digital, they are electronically transferable, unlike traditional handwritten signatures.[171] Digital signatures have other advantages over traditional signatures. In addition to authenticating the user's identity, a digital signature is able to authenticate the user's business traits.[172] For instance, the user's place of employment and level of authority can be authenticated.[173] Digital

---

economy. As proof of the worldwide concern over personal information and the Internet, in May 2000, the Federal Trade Commission recommended "that Congress pass a law that would regulate online privacy in four areas: notice, choice, access and security." *Id.* These four areas are also covered by the Amendment and Directive 95/46.

165. *See* discussion *supra* note 161 (discussing the ways a business can reorganize its structure, thereby falling within the small business exemption and becoming free from regulation of the Amendment).

166. Ann Cavoukian, *Privacy: The Key to Electronic Commerce* (Apr. 1998), *at* http://www.ipc.on.ca/english/pubpres/sum_pap/papers/e-comm.htm. Ann Cavoukian, Ph.D. is the Information and Privacy Commissioner of Ontario, Canada. *Id.*

167. *Id. See also* INQUIRY II, *supra* note 12, at 10.

168. *See* INQUIRY II, *supra* note 12, at 10.

169. *See* Cavoukian, *supra* note 166.

170. Roger Clarke, *Promises and Threats in Electronic Commerce* (Aug. 13, 1997), *at* http://www.anu.edu.au/people/Roger.Clarke/EC/Quantum.html [hereinafter *Promises and Threats*].

171. *See DigSig supra* note 12.

172. *Id.*

173. *Id.*

signatures are a form of algorithmic asymmetric cryptography.[174] A digital signature is a "message digest," or the encrypted form of the sender's original message.[175] The sender will encrypt the message using a private key, and the recipient decodes the message using the public key.[176] Once the message is decoded, the recipient can, using the public key, recreate the message digest and compare it to the original digital signature.[177] If the two digital signatures are identical, the recipient can be positive that the contents of the message received are the same as those allegedly sent, and the alleged sender was the only individual who was able to send such message.[178] Consequently, the sender cannot deny sending the message.[179]

Digital signatures, like any other technology that sends personal information over the Internet, are susceptible to unauthorized individuals using the sender's personal information.[180] Therefore, for individuals who are apprehensive about sending personal information over the Internet there is an alternative method of privacy protection called electronic cash or virtual money ("e-cash").[181] Instead of transmitting identifiable personal information over the Internet, the individual sends e-cash or tokens.[182] E-cash works just like traditional cash because the individual can enter into commercial transactions without providing any personal information, and thus, not revealing their identity.[183] In terms of privacy, e-cash is the most

174. *Id.* As the name indicates, asymmetric cryptography involves the use of two distinguishable, but related "keys." *Id.* The key is the tool by which messages are "locked or encrypted." *Id.* The sender of the message uses a "private key" to encrypt the message they wish to send, and the recipient of the message can "unlock or decrypt the digital signature by using a public key." *Id.* Theoretically, only the sender has access to the private key which is unique to that individual, much like a handwritten signature, or a fingerprint. *See Promises and Threats, supra* note 170.

175. *See DigSig, supra* note 12.

176. *See Promises and Threats, supra* note 170.

177. *See DigSig supra* note 12.

178. *Id.*

179. *Id.*

180. *See* Cavoukian, *supra* note 166 (discussing two risks associated with digital signatures).

181. *See id.*

182. *Id.*

183. *Id.*

protective mode of electronic commerce, as it prevents the collection, use and disclosure of the individual's personal information.[184] In addition, it is arguable that the use of e-cash necessarily renders moot the standards set in the Amendment.[185] This is not necessarily the fault of Parliament; rather, it is an example of the exponential rate at which technology grows. In this situation, the technology grew to protect the privacy concerns of the individual. However, there is nothing to prevent business organizations from utilizing technologies that allow them to participate in legal acts by rendering statutory schemes obsolete.

VIII. CONCLUSION

In an increasingly global and computer based world economy, the protection of private information on the Internet concerns every aspect of commerce, the individual, business and government. Legalization of deceptive business practices at the expense of the individual's privacy will only undermine the trust necessary between the individual and business to maintain and promote efficient electronic commerce. Furthermore, a lack of trust will arguably have a detrimental effect on electronic commerce. The ideal solution to this problem is for the individual, the business and the government to act responsibly and protect both the privacy concerns and economic interests that arise when the Internet is used for commercial purposes. This Note has proposed that the Australian government's attempt to protect privacy in the private sector is nothing more than a pretext for the promotion of the Australian Internet in the world economy. At this juncture, it appears that the individual's privacy will be effectively protected only through the utilization of technologies, such as digital signatures, in the private sector. Thus, the individual must take it upon himself

184. *Id.*

185. Although e-cash does not require the transfer of personal information, this technology is not without its problems. E-cash is subject to counterfeiting, or the "double spending problem." Jim Miller, *Answers to Frequently Asked Questions About Electronic Money, or E-Money, and Digital Cash, at* http://www.ex.ac.uk/~RDavies/arian/emoneyfaq.html (last visited Feb. 23, 2002).

or herself to use such technologies and elect government officials who will put a premium on privacy.

Matthew Kohel[*]

* The author will be receiving his J.D. from Brooklyn Law School in June 2002. He would like to thank his family for their love and support throughout his education.