EXPORTING TRUST: DOES E-COMMERCE NEED A CANADIAN PRIVACY SEAL OF APPROVAL?

JOHN MACDONNELL*

It has been suggested that Canada should develop a consumer protection seal, or trustmark, for placement on web sites as an assurance that privacy is not at risk in the on-line environment. This article explores whether a Canadian trustmark would be redundant in light of the Personal Information Protection and Electronic Documents Act.

Consumers are sceptical about surrendering personal information online when it can so easily be collected, used, and disclosed for purposes beyond their control. Data protection laws have been around since the early 1970s, but the Internet's mass acceptance has added new urgency to their development and spread.

The author contrasts the protection offered by the Act *with the policies of three high-profile trustmark programs to better understand where the legislative and self-regulatory approaches merge and diverge. He makes a proposal for a Canadian trustmark that uses the federal law as a starting point, but, at the same time, embraces more consumer-oriented and Internet-aware policies. Bringing this program to the international stage would be a priority because there is little point in restricting such an effort to one country.*

Il a été suggéré que le Canada développe un sceau de protection ou une marque de confiance pour les consommateurs qui serait affichée sur les sites Web en tant que garantie que la vie privée n'est pas compromise dans l'environnement en ligne. Cet article examine si une marque de confiance canadienne est superflue à la lumière de la Loi sur la protection des renseignements personnels et les documents électroniques.

Les consommateurs hésitent à donner des renseignements personnels en ligne par ce qu'il est si facile de recueillir, d'utiliser et de diffuser ces renseignements pour des raisons hors de leur contrôle. Les lois sur la protection des données existent depuis le début des années 1970, mais l'acceptation en masse d'Internet a ajouté une dimension d'urgence à leur développement et diffusion.

Cet article démarque la protection offerte par la Loi des politiques de trois programmes de marques de confiance de renommée pour mieux comprendre où les démarches législatives et d'auto-réglementation s'entendent et divergent. L'auteur suggère l'adoption d'une marque de confiance canadienne qui utilise la loi fédérale comme point de départ, mais qui en même temps s'inspire davantage de politiques axées sur les consommateurs et une sensibilisation à Internet. Il serait urgent de présenter un tel programme sur la scène internationale parce qu'il semble futile de limiter de tels efforts à un seul pays.

TABLE OF CONTENTS

I. INTRODUCTION 347
II. THE TRUST SHORTAGE 350
III. THE PRIVATE WHY 356
A. THE AMERICAN EXPERIENCE 360
B. THE CANADIAN EXPERIENCE 362
IV. TRUSTMARKS IN THE DATABASE NATION AND BEYOND 366
A. THE *PIPA* PARED DOWN 372
B. FALLING SHORT OF THE MARK 376

* This article was submitted by John MacDonnell in partial fulfilment of the requirements for the degree of Master of Electronic Commerce at Dalhousie University. It was written under the supervision of Professor Teresa Scassa, who the author would like to thank for her time and advice. Professor Michael Deturbide also provided useful commentary while acting as a reader. The author would also like to acknowledge the support of his wife, Sherri MacDonald.

C. SURPASSING THE MARK 381
V. DEVELOPING A CANADIAN SEAL 385
A. TAKING THE INTERNATIONAL STAGE 394
VI. CONCLUSION 395
APPENDIX 1: THE OECD GUIDELINES 398
APPENDIX 2: THE FTC'S FIPS FOR THE WEB 399
APPENDIX 3: SCHEDULE 1 OF THE *PIPA* 400
APPENDIX 4: BBBONLINE 408
APPENDIX 5: TRUSTE 421
APPENDIX 6: WEBTRUST 434

I. INTRODUCTION

In January 2000 the Canadian E-Business Opportunities Roundtable[1] identified six areas in which Canada should strive to establish e-business leadership. The sixth goal is to build a global reputation regarding Internet policy development "by establishing a Canadian-branded, internationally recognized consumer protection mark and forum for dispute resolution."[2]

The stated goal of the Roundtable is that the development of the consumer protection mark, or trustmark, be led by the private sector through consultation with interested parties such as the retail business sector, consumer groups, government, and the Canadian Standards Association ("CSA") International. CSA is the standards body whose *Model Code for the Protection of Personal Information*[3] is the core of recent federal privacy legislation. Once established in Canada, the trustmark would be transformed quickly "into an international standard providing a higher level accreditation recognized across borders."[4] The Roundtable foresees the mark being managed by a neutral third party tasked to build awareness, promote adoption of the program, track compliance, and provide a system for dispute resolution.

This article considers the merits of developing such a trustmark, focusing particularly on privacy issues. Although trustmarks that give assurances on a variety of matters, from fraud protection[5] to merchant reliability,[6] have been developed for the on-line

---

1 The Roundtable is an initiative of The Boston Consulting Group (Canada). In mid-1999, it drew together participants from the federal government and the private sector to examine ways to better position Canada to take an international leadership role on e-commerce issues.

2 The Boston Consulting Group (Canada), "Fast Forward: Accelerating Canada's Leadership in the Internet Economy" January 2000 at 9, online: Industry Canada <http://e-com.ic.gc.ca/english/documents/roundtable.pdf> (date accessed: 2 December 2000).

3 CSA International, "Model Code for the Protection of Personal Information," CSA Standard CAN/CSA-Q830-96, online: Canadian Standards International <http://www.cga.ca/standards/privacy/code/> (date accessed: 8 July 2001) [hereinafter "Model Code"]. In a slightly different version, it appears in the federal legislation as Schedule 1 to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, online: Department of Justice <http://laws.justice.gc.ca/en/P-8.6/79968.html> (date accessed: 7 July 2001) [hereinafter "Schedule 1"].

4 Boston Consulting Group (Canada), *supra* note 2 at 42.

5 See *e.g.*, the SquareTrade Seal Program, which promises to refund up to $250 US of a consumer's money if a merchant does not deliver as promised. SquareTrade Seal Program, online: <http://www.squaretrade.com/learnmore/seal_092100.jsp> (date accessed: 4 December 2000).

environment, the privacy of personal information is usually either the core issue or is inextricably linked to the others. Since a growing number of institutions are entering the field,[7] there should be sound reasons for a new Canadian entrant. If it would simply be reinventing the wheel or, worse still, muddying the waters for consumers faced with a plethora of trustmarks, the necessity of this endeavour would seem to be in doubt.

Another important factor is the *Personal Information Protection and Electronic Documents Act*,[8] ("*Act*") which took partial effect on January 1, 2001. At the same time as the Canadian E-Business Opportunities Roundtable was delivering its report, Parliament was considering and subsequently passed Bill C-6, as the *Act* was known in the national legislature. The provisions in Part 1 and Schedule 1 of the *Act* regarding the collection, use, and disclosure of personal information by organizations engaged in commercial activity would have to be accounted for in any Canadian-based trustmark program. In fact, the passing of the *Act* could be seen as a major setback to the idea because it establishes basic, legally enforceable privacy protections. Why bother placing a trustmark on a web site if the government has stepped in as the guardian of citizens' privacy?

It is unlikely, however, that the advent of the *Personal Information Protection Act* ("*PIPA*")[9] makes a trustmark unnecessary here. Since on-line activity does not respect borders, Canadians are quite likely to conduct business with a web site in a jurisdiction that need not concern itself with the *PIPA*. In a global marketplace, a trustmark may act as a shorthand way of alerting consumers that a particular site meets or exceeds Canadian legal expectations. The *PIPA* itself may be suitable only as a baseline for the trustmark envisioned by the Roundtable, which could strive for a higher standard. The trustmark's presence would be beneficial when it appears on a foreign site, reassuring the visitor that the same standards apply there as at home. Likewise, people of other nationalities who encounter the trustmark might come to regard it as a beacon offering a way to safely navigate the sometimes precarious privacy waters of the World Wide Web ("Web").

TRUSTe,[10] Better Business Bureau Online ("BBBOnLine"),[11] and WebTrust[12] are three trustmarks that already have some standing in the on-line marketplace. If they meet or exceed the requirements of the *PIPA*, there would be less justification for another

---

6 WebAssured, for instance, offers background information on a company, such as its physical address, annual sales, and history of complaints, when consumers click on the seal associated with the program. WebAssured, online: <http://www.webassured.com/merchant/faq.cfm> (date accessed: 4 December 2000).

7 For a list which is by no means comprehensive, see Internet Seals, which is maintained by the Privacy Council. Privacy Council, "Internet Seals," online: Privacy Council <http://www.privacy council.com/links_ iseals.htm> (date accessed: 4 December 2000).

8 S.C. 2000, c. 5, online: Department of Justice <http://laws.justice.gc.ca/en/P-8.6/index.html> (date accessed: 23 June 2001).

9 The *PIPA* refers only to Part 1 and Schedule 1 of the *Personal Information Protection and Electronic Documents Act*, which in Parts 2 through 5 facilitates the acceptance of e-commerce by giving legal recognition to electronic signatures and electronic documents.

10 TRUSTe, online: TRUSTe Homepage <http://www.truste.com> (date accessed: 23 June 2001).

11 BBBOnLine, online: BBBOnLine Homepage <http://www.bbbonline.com> (date accessed: 23 June 2001).

12 WebTrust, online: WebTrust Homepage <http://www.webtrust.org> (date accessed: 23 June 2001).

entrant into this field. In a recent study,[13] all of them were found to be playing a valuable role in the promotion of privacy. At the same time, they fell short[14] of the standards set by the Organisation for Economic Co-operation and Development ("OECD") in the 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[15] It seems unlikely that they would fully meet the requirements of the *PIPA* since the *Act* incorporates CSA International's Model Code, which is based on the OECD *Guidelines*. Some privacy advocates believe that the OECD's work is itself in need of an overhaul because it predates the popular acceptance of the Internet and fails to anticipate some of the challenges posed by this new medium.[16]

This article examines whether these three trustmarks meet the standard set by the *PIPA*. Even if they do not meet it, their positions as first movers in the e-commerce marketplace could make global acceptance of a Canadian branded trustmark that much more difficult. All three have primarily American origins. They first appeared in the United States because of its role as the birthplace of e-commerce and the deep-rooted belief in the US that industry self-regulation is more efficient than government oversight. The hole in the marketplace created by this laissez-faire attitude led to a perceived need for these services. However, if this country becomes known as a standard-bearer for fair information practices, a trustmark with impeccable Canadian credentials may carry more weight at home and abroad than one of American lineage.

Before delving into a consideration of the trustmarks themselves, Part II of this article first addresses the specific conditions surrounding business-to-consumer e-commerce that create a demand for them. Cyberspace is set apart from "meat space" because of the ease with which visitors can be trailed and information about them collected for correlation with other bits that have been amassed from sources, both online and off. What if every consumer walking through a mall was stamped with a Universal Product Code ("UPC"), that arrangement of machine readable numbers and bars one sees on such things as milk cartons and book jackets? Then it would be possible to scan the UPC and enter each action of the consumer into a database. Consumers become the consumed as information about everyday activities is suctioned into a file for later perusal. Browsing online can be a lot like that. The question is one of awareness. People may not realize that they are in

---

[13] A. Cavoukian & M. Crompton, "Web Seals: A Review of Online Privacy Programs" (22nd International Conference on Privacy and Personal Data Protection, Venice, September 2000), online: Australian Privacy Commissioner <http://www.privacy.gov.au/publications/seals.pdf> (date accessed: 3 December 2000).

[14] *Ibid.* at 37.

[15] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (23 September 1980), online: OECD <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM> (date accessed: 24 October 2000) [hereinafter *Guidelines*] reproduced in Appendix 1.

[16] See M.D. Kirby, "Protection of Privacy and Human Rights in the Digital Age" *International Dimensions of Cyberspace Law*, (30 June 1998), online: Law and Justice Foundation of New South Wales <http://www3.lawfoundation.net.au/resources/kirby/papers/19980630_unespriv.html> (date accessed: 14 January 2001); and M.D. Kirby, "Privacy Protection — A New Beginning?" (21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999), online: Law and Justice Foundation of New South Wales <http://www3.lawfoundation.net.au/resources/kirby/papers/19990913_privacy.html> (date accessed: 14 January 2001).

a public place while online. As awareness grows, consumers may demand more control over what personal data about them is collected and how it is used.

Trustmarks are one answer to such demands, but they must be built upon the foundation of earlier thinking in the privacy arena. Part III of this article is a brief overview of developments since the late nineteenth century that have influenced current views on data protection and the privacy of personal information. A pattern emerges over the course of this discussion: New technologies lead to anxiety about their potential harmful effects on personal privacy. Calls to somehow regulate the new technology are resisted but eventually heeded. In the e-commerce arena, the United States has been the jurisdiction most keenly interested in avoiding the legislative route. However, signs are emerging that trustmarks have only been partially successful as a tool for industry self-regulation. Their continued role in e-commerce may be as a helpmate to legislation rather than a substitute.

Part IV is the aforementioned examination of the TRUSTe, BBBOnLine, and WebTrust trustmark programs in relation to the *PIPA*. Part V discusses the prospects for a Canadian trustmark program. It is proposed that the office of the federal privacy commissioner would be a natural body to play a lead role in the endeavour. In order to transform the effort into a global initiative, it should then be taken over and further developed by an international coalition of data protection offices.

II. THE TRUST SHORTAGE

It is widely accepted that a lack of trust is one of the major obstacles to the further growth of e-commerce. A variety of studies[17] have proclaimed this problem, and trustmarks are simply one solution that has been proposed. Other solutions include legislative action and technical aids such as the Platform for Privacy Preferences ("P3P").[18]

While Europe and Canada have been quicker to legislate, the anti-regulatory fervour in the United States has slowed the process in that country. This is significant because the United States is the engine that has been moving e-commerce along at such a rapid rate. Because of its central role in the commercialization of the Internet, much of the research on consumer views about privacy and trust has an American focus. It is interesting to note that even in the bastion of free enterprise, the aura around e-commerce is one of mistrust,

---

[17] As well as the studies cited below, see also the UCLA Center for Communication Policy, "The UCLA Internet Report: Surveying the Digital Future" 25 October 2000 at 45, online: UCLA Center for Communication Policy <http://www.ccp.ucla.edu/pages/internet-report.asp> (date accessed: 29 October 2000). Concern about privacy of personal data was found to be the number one worry about shopping online.

[18] P3P is an emerging standard that would allow web sites to translate their privacy policies into a machine-readable format to be automatically read by the browser of a visitor to the site. The browser informs the visitor about whether the policies meet their pre-set privacy expectations. Further information is available online: Platform for privacy preferences initiative, Privacy Preferences Project Homepage <http://www.w3.org/P3P/> (date accessed: 23 June 2001).

not trust. In a study released in June 2000,[19] Americans and Canadians were asked to agree or disagree with the statement "I am very reluctant to give out my personal information while shopping online." Fifty-nine percent of the time, American respondents who had made on-line purchases in the past either strongly or somewhat agreed with the statement.[20] In Canada levels of apprehension were even higher, with 65 percent of Canadian respondents strongly or somewhat agreeing.[21]

The same statement was also put to people who had browsed for goods online but had not ever bought anything. Unsurprisingly, their reluctance was greater than that among the first group. Of the Canadian respondents, 74 percent agreed strongly or somewhat agreed. In the United States 62 percent of consumers gave the same response.[22]

This mistrust is born of the fear that personal information will be distributed beyond its intended purposes and beyond the control of the people by whom it was supplied. According to a study of 1,017 American Internet users released in August 2000, 86 percent of the respondents were concerned that personal information about them or about their families could find its way to businesses or to people that they did not know.[23] The same percentage of respondents favoured opt-in privacy policies requiring organizations to seek explicit permission before gathering any personal information.

In this context, it is important to consider what constitutes personal information and, more precisely, personal identifying information. The United States Federal Trade Commission ("FTC") places name, postal address, and e-mail address in the latter category.[24] According to the Commission, personal information is a broader class that includes personal identifying information plus demographic information (*e.g.*, age, gender, education level, income) and preference information (*e.g.*, hobbies, interests).[25] In this age of networked databases, however, the FTC may be too conservative. According to one commentator, it is possible to uniquely identify 87 percent of the American population

---

19 The Boston Consulting Group, "Winning the Online Consumer in Canada: Converting Browsers into Buyers" June 2000, online: The Boston Consulting Group <http://www.bcg.com/media_center/BCG_Canadian_Consumer.pdf> (date accessed: 16 October 2000). Despite its title, this study polled American and Canadian consumers.

20 *Ibid.* at 12.

21 *Ibid.*

22 *Ibid.*

23 S. Fox, "Trust and Privacy Online: *Why Americans Want to Rewrite the Rules*" (The Pew Internet and American Life Report, 20 August 2000), online: Pew Internet and American Life Project <http://www.pewinternet.org/reports/toc.asp?Report=19> (date accessed: 17 October 2000).

24 United States, Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) at 20, online: Federal Trade Commission <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (date accessed: 27 October 2000).

25 Under the *PIPA*, *supra* note 8, part 1, s. 2(1), personal information is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." There is no use of the FTC's narrower phrase "personally identifying information." The various trustmarks also define one or both phrases in various ways. How these terms are defined in legislation and policy provides the basis for just what data is regulated, and what data may be freely collected, used, and disclosed.

starting with only an individual's date of birth, gender, and postal ZIP code.[26] This information is exactly the type of apparently trivial data that web sites collect[27] and individuals, thinking that it is of little consequence, may provide. Not one of those three items would be considered to be personal identifying information by itself, but taken together they can identify a previously anonymous individual.

Considering the above, it is no wonder that some people may be classified as privacy protectionists who will balk at providing data to web sites. Studies have placed the percentage of Internet users in this category at 17 percent[28] to 27 percent.[29] Still, the majority of Internet users, over 50 percent, are classified as privacy pragmatists[30] and are willing to provide information under the right circumstances. A third group, which one study[31] identifies as the "marginally concerned," would provide information to web sites under almost any circumstances. However, there are situations in which even the marginally concerned would like their privacy respected.[32]

One way to discover how a web site's operators claim to deal with personal information is by reading the site's privacy policy. Posting such a policy has become a common, though not universal, practice.[33] However, there is wide variation in their content and visibility. Further, unless it has been well drafted, it is unlikely that the average user would fully read a policy. Some sites now post two versions, one short policy written in plain language, and a second, more comprehensive version composed in legal terminology. In theory, trustmarks take the notion of policy simplification a step further by associating an icon with the privacy practices of a site. If one knows what the icon means, there is less need to scrutinize the policy.

An example of a clearly written privacy policy may be found at Amazon.com, one of the best known e-tailers. Its clarity ensures that a startling clause towards the end does not

---

26 The commentator, Latanya Sweeney, an assistant professor of computer science and public policy at Carnegie Mellon University, is quoted in an article by Erik Sherman. E. Sherman, "It doesn't take much to make you stand out" *Newsweek* 136:16 (16 October 2000) 74N.

27 The FTC found that 99 percent of its sample of the busiest American commercial sites collected an e-mail address or some other personally identifiable piece of information. The figure was 97 percent for a random sample consisting of 335 sites. The commission concluded that most of the surveyed sites "are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior or surfing behavior information they collect to personal identifying information." See United States, Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) at 9-10, online: Federal Trade Commission <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> (date accessed: 27 October 2000).

28 L.F. Cranor, J. Reagle & M.S. Ackerman, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy" (14 April 1999), online: AT&T Labs-Research <http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm> (date accessed: 7 July 2001).

29 Fox, *supra* note 23.

30 The Cranor and Fox studies, *supra* note 28 and note 23, support this.

31 Cranor, *supra* note 28.

32 Being able to request removal from marketing mailing lists rates highly, for instance.

33 In its 2000 on-line privacy survey, the FTC calculated that 82 percent of commercial American web sites post a privacy policy. The figure is higher still when considering only the most popular sites. See United States, Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, *supra* note 27 at 10.

go unobserved: "This Notice and the Conditions of Use will change also, and use of information that we gather now is subject to the Privacy Notice in effect at the time of use."[34] In other words, no matter what the policy says now, the company reserves the right to change it and treat personal information collected before an amendment under the new rules, which should nullify any comfort one might take from the preceding statements.

In contrast, the policy in place at the WebMD site states: "We will notify you by email of any significant changes and obtain your 'opt-in' consent to any significant new uses of your Personal Information."[35] Perhaps, as a medical site, the operators are more attuned to the privacy concerns of site users than the bookseller appears to be. The site also undertakes to notify users of any "substantial" changes to the policy.[36] Unfortunately, the WebMD site is the exception. Many other sites, like Amazon, simply urge consumers to check back "frequently" in case their policy changes.[37] It is no wonder that there is mistrust surrounding e-commerce when many merchants reserve the right to alter the rules at any time, without notice. A poll of 580 Canadian Internet users released in January 2001 ably demonstrates this atmosphere of suspicion. Forty percent of the respondents did not believe that on-line companies would honour their posted privacy policies.[38] However, 70 percent said that the presence of a third party trustmark ensuring oversight of privacy policies would make them more likely to do business with a company.[39]

This discussion has centred on instances in which information is provided consciously and voluntarily, such as ordering merchandise, registering at a web site, or entering an on-line contest. Yet the very act of surfing the Web leads to the unwitting disclosure of information. This information can be meshed with prior data from previous registrations or contest entries to obtain a more complete picture of an individual. Many web sites use *cookies*. Cookies are small bits of text stored on a user's computer that enable the recognition of repeat visits from a single computer, allowing settings particular to that user to be maintained. A second function of cookies is to allow the particular computer that is visiting the site to be uniquely identified and tracked over a session or over multiple visits. This function allows for the acquisition of data about exactly which links are clicked and which pages are viewed.[40] This recording of clickstream data allows a site's operators to monitor usage patterns and better tailor pages to the interests expressed

---

34 Amazon.com Privacy Notice 2000, online: Amazon.com <http://www.amazon.com/exec/obidos/tg/browse/-/468496/> (date accessed: 10 November 2000).

35 WebMD Privacy Policy 2001, online: WebMD <http://my.webmd.com/privacy_policy> (date accessed: 7 July 2001).

36 *Ibid.*

37 *Supra* note 34.

38 D. Akin, "Canadians Still Not Sold On Net Privacy Policies" *The National Post* (17 January 2001) C6.

39 *Ibid.*

40 Other information gathered includes the time and duration of visits to a site, the Uniform Resource Locator ("URL") of the page from which a visitor linked to the site, and query terms entered into search engines.

by the user or users of a particular computer.[41] Most notably, on-line shopping is more difficult without the identifying link provided by cookies because each page request appears to come from a new customer. There is nothing to connect the Margaret Atwood novel selected for purchase on one page with the Stephen King blockbuster chosen on the next. This problem, known as "statelessness," can be addressed without using cookies; however, the solution is less secure. For instance, the electronics retailer Future Shop[42] switched to the use of cookies on its site in November 2000 after it was discovered that in some cases unauthorized people could log on and view other people's account details: name, address, phone number, and possibly credit card number.[43] Ironically, the much maligned cookie would have prevented a breach of security and an invasion of privacy.

Cookies play an important role in customizing sites and tracking users within a site. However, privacy advocates have become concerned with the third common use of cookies: building on-line profiles by tracking an individual computer across multiple sites on behalf of an advertising network.[44] DoubleClick, the most prominent of these companies, is said to have amassed 100 terabytes of information[45] and about 100 million consumer profiles.[46] Thus, while at a web site on which they might not object to the use of cookies because it allows for greater personalization, a visitor may also expose data to networks such as DoubleClick,[47] Engage, or 24/7 Media that control the advertisements on the site. Cookies belonging to the advertising networks are placed on the computers of site visitors even if they never click on an advertisement. This is done without notification — and is often not mentioned[48] in the privacy policies of the web sites

---

41 Amazon.com offers an example of this through a feature called "See more in the Page You Made," which operates when cookies are enabled. After browsing several pages on the site, every page thereafter has a link that, when clicked, takes the user to a page displaying links to all other recently visited pages on the site and a list of suggested links that may also appeal based on those previous choices.

42 Future Shop, online: Future Shop Homepage <http://www.futureshop.ca> (date accessed: 23 June 2001).

43 T. Hamilton, "Price Snafu Stings Web Retailer" *The Toronto Star* (17 November 2000) C01.

44 For a full discussion of this issue, see United States, Federal Trade Commission, *Online Profiling: A Report to Congress* (June 2000) Part 1, online: <http://www.ftc.gov/os/2000/06/onlineprofiling reportjune2000.pdf> (date accessed: 8 November 2000) and Part 2, online: Federal Trade Commission<http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>(dateaccessed:28November2000).

45 D. Hawkins, "Internet Privacy: Tracking the Web of Data You Weave" *U.S. News* (2 October 2000), online: USNews.com <http://www.usnews.com/usnews/issue/001002/nycu/privacy3.htm> (date accessed: 2 October 2000). One terabyte is enough to hold all the text in about two million Harlequin Romances.

46 H. Green, "Privacy: Outrage on the Web" *Business Week* (14 February 2000), online: Business Week online <http://www.businessweek.com/2000/00_07/b3668065.htm> (date accessed: 6 November 2000).

47 In the first quarter of 2001 DoubleClick served 181 billion advertisements. With numbers like that, it would be hard to believe that the average Web user would *not* run into a DoubleClick advertisement, let alone multiple DoubleClick advertisements. See DoubleClick, "DoubleClick Delivers on Q1 Expectations" (12 April 2001), online: DoubleClick <http://www.doubleclick.net/us/ corporate/presskit/press-releases.asp> (date accessed: 12 April 2001).

48 In its 2000 survey, the FTC found that the majority of commercial American web sites allow the placement of third party cookies. Furthermore, a majority of those sites made no disclosure of that fact to consumers. See United States, Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, *supra* note 27 at 21.

displaying the advertisements, which may, nevertheless, provide information about their own use of cookies. In response to complaints about this third party cookie activity, Netscape has implemented a setting in its Navigator browser allowing users to reject cookies other than those of the server from which the page originates.[49] Users may also choose to block cookies from individual sites, rather than all or none. Microsoft's Internet Explorer intended to follow suit, but this plan has been abandoned in favour of supporting P3P in Version 6 of the browser.[50] These are the two most popular browsers,[51] and they have long offered the ability to opt out of cookies entirely. However, offering this lessens their functionality at some sites and requires users to change the default cookies-on settings of which many are probably unaware. In fact, less than half of Internet users surveyed (43 percent) knew what a cookie was when asked in a recent survey.[52] Only 10 percent of those surveyed said that they had set their browser to block cookies.[53]

Nonetheless, cookies are better known than a related method of tracking web site visitors. This other method is known variously as web bugs, web beacons, clear Graphics Interchange Format ("GIF"),[54] or invisible GIFs. Generally only one pixel by one pixel in size and transparent, a web bug is invisible to the eye because it is tiny and blends into the background on a web page or in a Hypertext Markup Language ("HTML") e-mail message, which appears as a web page in an e-mail client.[55] Unlike third party cookies, which are associated with an advertisement on a page, web bugs can be placed on pages without advertisements. The only evidence as to its presence is found by looking at the source code for the page or message, and discovering that the web bug image loads from a different server than everything else. Typically, this third party server might belong to an advertising network that uses it to obtain information such as:

- The IP address of the computer that fetched the Web bug
- The URL of the page that the Web bug is located on
- The URL of the Web bug image
- The time the Web bug was viewed

---

49 Advertisers can work around this by sending their cookies from the same domain as the site being visited.

50 Privacy Foundation, Press Release "Microsoft Crumbles on Cookie-Blocking" (28 December 2000), online: Privacy Foundation <http://www.privacyfoundation.org/privacywatch/report.asp?id=51&action=0#microsoft> (date accessed: 22 June 2001).

51 As of June 2000, Internet Explorer had 86 percent of the browser market globally and Netscape had most of the remainder. Bloomberg News, "Short Take: Microsoft browser lead widens" (26 June 2000), online: CNET News.com. <http://news.cnet.com/news/0-1006-200-2154356.html> (date accessed: 14 November 2000).

52 Fox, *supra* note 23.

53 If the cookie preferences in browsers came with "off" as the default, then consumers would be able to opt in to their use. The browser makers would certainly not shy away from educating users on how to do this.

54 The Graphics Interchange Format is one of the most common file formats for graphics displayed on the Web.

55 R. Smith, "FAQ: Web Bugs" (August 2000), online: Privacy Foundation <http://www.privacyfoundation.org/resources/webbug.asp> (date accessed: 22 June 2001).

- The type of browser that fetched the Web bug image
- A previously set cookie value[56]

It is this last use of a web bug that causes concern.[57] The cookie links the bug and the information it has gleaned back to the on-line profile associated with that cookie. This process allows the network to associate the information in the profile with the visit to the bugged page, something the consumer is unaware of and may oppose if informed of the practice. In addition, web bugs in HTML e-mail can be used, among other things, to tell if an e-mail has been read or forwarded to another person within an organization.

In 1999 an Internet privacy advocate diminished the credibility of companies amassing on-line profiles by publicizing the existence of web bugs.[58] It was simply one of a series of revelations that furthered the case for legislation in the United States by showing the failure of self-regulation. In another instance, free jukebox software downloadable from the company RealNetworks was discovered to be tagging users with a unique identification ("ID") and then transmitting the information back to the company without the consumer's knowledge.[59]

It is this lack of notice about what and how information is being gathered that fuels the calls for legislation in the United States. Although there are legitimate uses for technology such as web bugs,[60] the failure to inform consumers understandably heightens the mistrust evident around e-commerce when the public does become aware of what is happening.

III. THE PRIVATE WHY

One of the most enduring and brief legal definitions of privacy is "the right to be let alone," which originated in the writings of Judge Thomas McIntyre Cooley,[61] a noted American jurist. However, the justice of the Michigan Supreme Court was referring to protection from threats of bodily harm. Two other writers, lawyers Samuel Warren and Louis Brandeis, adopted the phrase in 1890 and used it in their seminal article entitled

---

56 *Ibid.*

57 For a theory on how web bugs can be used by a "hacker" to open a big security hole in a user's computer, see T.C. Greene, "Fun With Internet Bugs" *The Register* (13 December 2000) online: The Register <http://www.theregister.co.uk/content/6/15423.html> (date accessed: 16 January 2001).

58 R. O'Harrow Jr., "Fearing a Plague of 'Web Bugs': Invisible Fact-Gathering Code Raises Privacy Concerns" *The Washington Post* (13 November 1999) E01.

59 S. Carberry, "Real Software's Privacy Gaffe: Learn More About the Finding That Made Privacy Groups Reel" *Smart Computing Guide Series* 8:4 (April 2000) 116 at 116-17.

60 A bug placed on a web site can allow for an independent accounting of visitors to a page. For an account of how using them to verify web site traffic numbers may be more privacy friendly than using server log files, see G. Mariano, "Web bugs draw interest of online traffic auditors" *CNET News*.com (29 January 2001), online: CNETNews.com <http://news.cnet.com/news/0-1005-200-4638938.html> (date accessed: 30 January 2001).

61 T.M. Cooley, *Cooley on Torts*, also known as *A Treatise on the Law of Torts, or, the Wrongs Which Arise Independent of Contract* (Chicago: Callaghan and Company, 1880). At 29, Cooley writes, "The right to one's person may be said to be a right of complete immunity: to be let alone."

"The Right to Privacy."[62] Here they argued for the recognition of a right to privacy from the intrusiveness of the media and "numerous mechanical devices [that] threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[63]

The struggle between technology and privacy had clearly begun and would intensify over the next century. Justice Brandeis famously re-entered the conflict almost forty years later to issue a dissenting opinion in a United States Supreme Court ruling on wiretapping.[64] He submitted that this technology was being used unwisely by the government and that it was a new threat to privacy. He referred to privacy as "the most comprehensive of rights and the right most valued by civilized men."[65]

This pattern of technology bringing new benefits, while simultaneously offering innovative ways to breach privacy, would be repeated through the decades. Most often, the presumption was that the entity likely to be abusing citizens' rights would be an arm of the government. The warnings increased in the 1960s as information processing became possible on an unprecedented scale because of the widespread adoption of the mainframe computer. In 1967 Alan F. Westin published a very influential book[66] examining how this data gathering, along with such developments as the extension telephone, miniature cameras, and minature microphones had the potential to erode privacy. Westin attempted to better understand privacy and offered a broader definition than did his predecessors:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[67]

This definition has been widely embraced and appears in judgments rendered by the highest courts in the United States[68] and Canada.[69] Unlike the passive nature of a "right to be let alone," this way of examining privacy foresees that the affected person or organization can play an active role in safeguarding their personal information. Personal data are not to be harvested without regard to the wishes of the individual. Instead, whoever is collecting, storing, using, or disclosing the information must engage in what have come to be known as fair information practices ("FIPs").

---

62 S.D. Warren & L.B. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193, online: Lawrence University <http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html> (date accessed: 28 September 2000). The phrase, "the right 'to be let alone'" appears at 195.

63 *Ibid.* at 195.

64 *Olmstead* v. *United States*, 277 U.S. 438 (1928).

65 *Ibid.* at 478.

66 A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

67 *Ibid.* at 7.

68 For example, see *U.S. Department of Justice* v. *Reporters Committee for the Freedom of the Press*, 489 U.S. 749 at 764 (1989), a case in which the media unsuccessfully tried to gain access to an FBI 'rap' sheet on a defence department contractor with ties to organized crime.

69 *R.* v. *Duarte*, [1990] 1 S.C.R. 30 at 46. The case considered whether electronic surveillance agreed to by one party to a conversation constituted a breach of an unwitting suspect's *Charter* right to freedom from unreasonable search and seizure.

A basic set of FIPs was established in 1973 with the publication in the United States of a five-part Code of Fair Information Practices.[70] The Code consists of:

1) Notice/Awareness: "There must be no personal data record-keeping systems whose very existence is secret";[71]
2) Choice/Consent: "There must be a way for an individual to find out what information is in his or her file and how the information is being used";[72]
3) Access/Participation: "There must be a way for an individual to correct information in his or her records";[73]
4) Security/Integrity: "Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse";[74] and
5) Enforcement/Redress: "There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent."[75]

These principles were codified in the public sector United States *Privacy Act of 1974*[76] and have been described as the "most significant American thinking on the topic of computers and privacy to this day."[77] However, they had less impact in their birthplace than they did in Europe.[78] Many European nations based omnibus laws on the principles that oversaw the protection of privacy in the public and private sectors. Data protection commissions were often established to enforce these laws.

Perhaps the best known set of FIPs was developed and released in 1980 by the Organisation for Economic Co-operation and Development. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[79] were among the first multinational efforts in this area. These eight interrelated and partly overlapping principles were created out of concern about automatic data processing[80] and the vast amount of personal information that can flow easily across borders.

---

70 Center for Democracy and Technology, "Comments on the Draft 'Principles for Providing and Using Personal Information'" (21 March 1995), online: Center for Democracy and Technology <http://www.cdt.org/privacy/comments_iitf.html> (date accessed: 25 October 2000).

71 *Ibid.*

72 *Ibid.*

73 *Ibid.*

74 *Ibid.*

75 *Ibid.*

76 *The Privacy Act of 1974*, 5 U.S.C. § 552a (1974), online: United States Department of Justice <http://www.usdoj.gov/foia/privstat.htm> (date accessed: 12 March 2001).

77 S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Cambridge: O'Reilly, 2000) at 7.

78 The German state of Hesse had enacted the world's first data protection statute in 1970. P.P. Swire, & R.E. Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (Washington, D.C.: Brookings Institution Press, 1998) at 22.

79 OECD, *supra* note 15. The *Guidelines* are reproduced in Appendix 1.

80 However, the *Guidelines* do not limit themselves to automatic data processing. They are technology neutral and deal with "the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes" (*ibid.* at para. 38).

However, it must be noted that this was not purely a move in favour of human rights. It was balanced by an equal or greater concern that the emergence of inconsistent data protection regimes in various nations might disrupt such economic drivers as the insurance and banking industries. Between 1973 and the release of the OECD *Guidelines*, many member countries of the organization had enacted legislation variously known as privacy laws, data laws, or data protection laws. Although the laws often had common features, their differences were seen as a potential barrier to the movement of data across international frontiers. The *Guidelines* were an attempt to introduce some minimum standards so that data processors could expect similar laws in different jurisdictions.

As the OECD was developing its *Guidelines*, a similar effort undertaken by the Council of Europe ("Council") resulted in the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.[81] The *Convention*, which came into force in 1981, had similar aims and means of achieving them. However, one essential difference is that the *Guidelines* are not legally binding on OECD member states, whereas the *Convention* is binding on the member states where it has been ratified. However, only 21 of the Council's 41 member states had ratified the *Convention* as of March 2001.[82]

Another significant difference is that the *Guidelines* avoid identifying any particular type of data that requires special care in its handling. The authors of the *Guidelines* state, "Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive."[83] At the same time, while creating an instrument that applies only to a limited geographic region, the Council names special data categories. These categories certainly reflect the European experience in World War II:

> Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.[84]

Regardless of the differences between the two instruments, the *Guidelines* and the *Convention* were the culmination of much of the thinking on the privacy front that occurred during the 1970s. They proved to be the source from which much of the world's data protection laws drew in the years that followed.

Yet in the late 1980s, the Commission of the European Union became concerned that the varied data protection laws in its member states posed a potential obstacle to the free flow of data across borders. The OECD *Guidelines* and the Council *Convention* had not had the desired effect of homogenizing data protection laws and so another tool was

---

[81] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, E.T.S. 108 (28 January 1981), online: Council of Europe <http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm> (date accessed: 19 December 2000) [hereinafter *Convention*].

[82] For the list of signatories see the Council of Europe, online: Council of Europe web site <http://conventions.coe.int/treaty/EN/searchsig.asp?NT=108&CM=8&DF> (date accessed: 26 October 2000). In the event that address changes, the information can be found via a search at Council of Europe online: <http://conventions.coe.int/>.

[83] See s. 19 a) of the Explanatory Memorandum in OECD's *Guidelines*, *supra* note 15.

[84] *Convention*, *supra* note 81 at Article 6: Special categories of data.

needed. This solution arrived in 1995 when the European Union ("EU") adopted the *Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data.*[85] The *Directive* goes beyond the OECD and Council measures because it is binding on the EU's 15 member states. More significantly, Article 25 restricts the transfer of data to non-member countries unless "the third country in question ensures an adequate level of protection."[86] This puts the onus on non-EU nations to examine their own data protection practices to ensure that they meet the standards of the *Directive*. The United States and Canada have taken different routes to achieve that end.

A. THE AMERICAN EXPERIENCE

In the United States, as in Canada until recently, there is no overarching privacy or data protection legislation in the private sector. The anti-regulatory stance of the American government towards the Internet was demonstrated in July 1997 when the White House released *A Framework for Global Electronic Commerce.*[87] The first of five principles listed in the *Framework* is that "[t]he private sector should lead" the development of electronic commerce. The section of the document on privacy[88] promotes the use of fair information practices and comments on the desirability of private industry working with consumer groups to develop a self-regulatory environment. However, there is a cautionary note at the end, with a reminder that this policy will be re-evaluated if effective privacy protection is not developed. That caution is a softened version of a message that precedes it by five paragraphs in which the administration warns that prompt action is needed to ensure that the privacy rights of children are not violated on the Internet. If not, "government action may be required."[89]

As it turns out, the Federal Trade Commission, in its 1998 report[90] to Congress, decided that self-regulation was not working to protect the privacy of children online. While studying 212 American commercial web sites aimed primarily at children aged 15 and under, the FTC found that 186 of them, or 88 percent, collected personal identifying information and 188, or 89 percent, collected personal information.[91] Only 109[92] of the 188 sites carried notice of even one of the commonly accepted FIP principles, and no site

---

85 EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] O.J. L. 281/31, online: The European Union <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html> (date accessed: 27 October 2000) [hereinafter *Directive*].

86 *Ibid.* at Chapter IV, Article 25, Principle 1.

87 The White House, *A Framework for Global Electronic Commerce* by W.J. Clinton & A. Gore (1 July 1997), online: United States Government Electronic Commerce Policy <http://www.ecommerce.gov/framewrk.htm> (date accessed: 10 March 2001) [hereinafter *Framework*].

88 *Ibid.* at II Legal Issues, Number 5 at para. 17.

89 *Ibid.* at II Legal Issues, Number 5 at para. 12.

90 United States, Federal Trade Commission. *Privacy Online: A Report to Congress*, *supra* note 24.

91 *Ibid.* at 31.

92 *Ibid.* at 36.

was reported to engage in the full range of fair information practices.[93] Because of these findings, the commission recommended that Congress develop legislation to put parents in control of the on-line collection and use of information from their children. The result was the *Children's Online Privacy Protection Act of 1998*,[94] which came into force on April 21, 2000. It dictates that web sites must obtain parental consent before collecting, using, or disclosing personal information of anyone younger than 13 years old.[95]

By May 2000, when the FTC launched its third report[96] to Congress regarding on-line privacy and the effectiveness of industry self-regulation, the Commission noted improvement. However, the improvement was not enough to ward off a call for legislation.[97] In a random sample of 335 American commercial web sites that collected personal identifying information, only 20 percent applied the first four fair information practices.[98] The figure was higher, 42 percent, when 91 of the 100 busiest commercial sites were considered. The Commission saw this as a failure of self-regulation and cited the lack of privacy seals, which it referred to as "key enforcement mechanisms,"[99] on the surveyed web sites as an indicator of this failure.

However, the reversal of the FTC on the legislation issue was not complete. In a scathing dissent to the report, one commissioner wrote that it was "embarrassingly flawed"[100] and called into question its presentation of facts, its analysis, and its conclusions. The vigorous dissenting opinion ends with a call to refrain from legislating or, if lawmakers must get involved, to limit the scope of legislation to the Notice principle.[101]

Despite the lack of unanimity within the Commission, a number of Internet consumer privacy bills were introduced during the 106th Congress. None of them passed before the

---

93 The Commission revises the FIP principles for children so that they involve 1) parental notice/awareness, 2) parental choice/consent, 3) access/participation, 4) integrity/security and 5) enforcement/redress.

94 15 U.S.C. § 6501 (1994).

95 *Ibid.*

96 United States, Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, *supra* note 27.

97 This was a reversal from the previous year's report which said, "the Commission believes that legislation to address on-line privacy is not appropriate at this time." United States, Federal Trade Commission, *Self-Regulation and Privacy Online* (July 1999) at 12, online: Federal Trade Commission <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (date accessed: 27 October 2000).

98 United States, Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, *supra* note 27 at 12. When the FTC refers to FIPs, it often means only the first four: Notice, Choice, Access and Security. This is because the fifth, Enforcement, is usually the duty of a third party that is not directly responsible for the first four. Appendix 2 contains the FTC's version of FIPs, rewritten for the Web as they appear on page 37 of *Privacy Online*.

99 *Ibid.* at 20. Fifty-five percent of the 91 most popular sites boasted a seal, but only 8 percent in the random sample did.

100 See O. Swindle, "Dissenting Statement of Commissioner Orson Swindle" in United States, Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace. Ibid.* at 1.

101 *Ibid.* at 26.

session adjourned, but there was discussion of the "inevitable"[102] success of such a bill as the 107th Congress began. While some business groups prepared for a battle,[103] others dropped their formerly antagonistic stance to privacy legislation.[104]

Interestingly, no one in the United States seems to talk about the role that on-line privacy legislation might play in helping American organizations comply with Article 25 of the EU *Directive*. The American solution to that problem was to negotiate a safe harbour agreement with the EU. Under the terms of the deal, which took effect on November 1, 2000, American companies can receive personal data of European origin if they agree to abide by detailed standards of notice, choice, access, and security.[105]

B. THE CANADIAN EXPERIENCE

Along with several other nations, Canada awoke to the privacy implications of the growing number of computerized databases in the late 1960s and early 1970s and decided to examine the issue in detail.[106] A Task Force on Privacy and Computers was struck and, following a year of work, it concluded that there was no imminent privacy crisis, as some had feared. However, a number of actions found to be worth considering included:

- Keeping a watchful eye on the amount of data about Canadians leaving the country while perhaps stemming the flow by encouraging local development of databanks;
- Establishing some sort of data oversight agency augmented by an ombudsman to handle specific complaints about privacy violations in areas such as health care; and
- Ensuring that government, "the principal collector and instigator of the collection of personal information," put its own house in order by having a central agency to regulate its databanks and develop codes of ethics to administer government-funded research.[107]

---

102 J. Gartner, "New Congress to Push Privacy" *Wired News* (7 January 2001) online: Wired News <http://www.wired.com/news/politics/0,1283,40965,00.html> (date accessed: 8 January, 2001).

103 D. McGuire, "US Chamber Vows to Fight Privacy Legislation" *Newsbytes* (9 January 2001) online: WashingtonPost.com <http://www.newsbytes.com/news/01/160268.html> (date accessed: 10 January 2001).

104 M. Mosquera, "AeA Reverses Policy, Backs Privacy Legislation" *TechWeb News* (18 January 2001), online: TechWeb <http://content.techweb.com/wire/story/TWB20010118S0014> (date accessed: 18 January 2001).

105 K. Perine, "EC Will Stand by 'Safe Harbor' Deal" *The Industry Standard* (27 July 2000) online: The Industry Standard <http://www.thestandard.com/article/display/0,1151,17197,00.html> (date accessed: 28 October 2000).

106 Canada, Department of Communications/Department of Justice, *Privacy and Computers* (Ottawa: Information Canada, 1972). At 226, the authors report similar studies already complete or in progress in Denmark, France, Germany, the Netherlands, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

107 *Ibid.* at 183-84.

Five years after the task force report, the federal government appointed its first privacy commissioner under the *Canadian Human Rights Act*.[108] On July 1, 1983, the government brought the *Privacy Act*[109] into force, the duties of the commissioner now falling under that legislation.[110] The *Privacy Act* empowers the commissioner to monitor the federal government's collection, use, and disclosure of citizens' and employees' personal data. It was not until June 1984, when the federal government committed itself to the OECD *Guidelines*, that momentum began to build to establish standards for the protection of personal information in the private sector. At that time, the Department of Justice was responsible for advising industry to comply with the *Guidelines* by adopting voluntary privacy protection codes. However, one need only read the annual reports of the privacy commissioner to see that hopes for the success of this approach dimmed with each passing year. In his 1988-89 report, the commissioner wrote of the "entirely sensible" voluntary approach to data protection in industry but concluded: "[I]t has become time for government to treat volunteering in this business much as 'volunteers' are traditionally found in the armed forces."[111] By the following year the commissioner was contemplating an amendment to the *Privacy Act* that would require federally regulated firms in industries such as air transport, telecommunications, and banking to develop and implement voluntary codes of privacy protection.[112] These would be submitted to the commission for review.

Despite increasingly stronger calls for some type of regulation, the situation was much the same the next year when a new privacy commissioner was in place. In his first annual report, Bruce Phillips submitted the following: "The issue now is not whether the private sector can continue without privacy codes, but how long it will be before compulsion in one form or another enters the equation."[113] It would be another nine years before Phillips, then presenting his last annual report before leaving the position, had an answer to the question posed within that statement. That answer was the *Personal Information Protection and Electronic Documents Act*,[114] which was enacted on April 13, 2000. Of course, it did not arrive fully formed. It developed slowly over the course of the previous decade, beginning with the work of the Canadian Standards Association, now CSA International, in 1991. The CSA formed a committee with representatives of business, consumers, labour, and government to develop a model privacy code for the private sector. In 1995 the federal government's Information Highway Advisory Council spoke favourably of the draft code while recommending legislation as the best course of action

---

108 *Canadian Human Rights Act*, R.S.C. 1985, c. H-6, online: Department of Justice <http://laws.justice.gc.ca/en/H-6/index.html> (date accessed: 22 June 2001).

109 *Privacy Act*, R.S.C. 1985, c. P-21, online: Department of Justice <http://laws.justice.gc.ca/en/P-21/index.html> (date accessed: 22 June 2001).

110 *Ibid.*, s. 53.

111 Canada, Privacy Commissioner of Canada, *Annual Report 1988-89* (Ottawa: Minister of Supply and Services, 1989) at 11.

112 Canada, Privacy Commissioner of Canada, *Annual Report 1989-90* (Ottawa: Minister of Supply and Services, 1990) at 14.

113 Canada, Privacy Commissioner of Canada, *Annual Report 1990-91* (Ottawa: Minister of Supply and Services, 1991) at 4.

114 *Supra* note 8.

to ensure privacy protection in the electronic environment.[115] Thus a report the next year announcing that the ministers of Industry and Justice would soon be proposing a legislative framework for data protection was not a surprise.[116]

Quebec had actually accomplished that feat at the provincial level in June 1993 when it passed *An Act Respecting the Protection of Personal Information in the Private Sector*.[117] Based on the OECD *Guidelines*, the law was the first comprehensive privacy legislation affecting the private sector adopted by any jurisdiction in North America. It would be several years before it was joined by similar legislation at the federal level.

The arrival of the *PIPA* grants Canadians the type of data protection that is commonplace in Europe but that is still being resisted in the United States. In essence, the *PIPA* turns the CSA *Model Code for the Protection of Personal Information*,[118] which was approved in 1996, into law. The Model Code is appended to the *Act* in Schedule 1, an unusual practice that has led to criticism because it was never designed to be law. The generality, which is a positive aspect of a voluntary code, conflicts with the need for greater specificity in legislation.[119] In fact, by absorbing the CSA Model Code, the *Act* leaves itself open to any criticism targeted at the code. One such complaint revolves around its concentration on what a critic refers to as *efficiency measures* as opposed to *limiting measures*.[120] These represent the two major functions of privacy principles and legislation: an ability to ensure that when surveillance takes place, it does so fairly and openly; and an ability to prevent surveillance altogether. Greenleaf's use of the word *surveillance* as opposed to *data collection* signals his sympathy for the position that the flow of personal information should be curtailed whenever possible.[121] He contends that the CSA Model Code and the OECD *Guidelines* concern themselves with the efficiency criteria, while not thoroughly addressing collection limitation. Unless restrictions are placed on what is collected in the first place, data protection laws can simply be ways to legitimize increased gathering of personal identifying information. Greenleaf argues that when organizations are given free rein to define the purposes of their information collection, they can sidestep legislation that limits the use of information to defined

---

115 Canada, Industry Canada, *Final Report of the Information Highway Advisory Council* (Ottawa: Industry Canada, August 1995), online: Industry Canada <http://strategis.ic.gc.ca/SSG/ih01070e.html> (date accessed: 28 November 2000). Privacy and security are addressed at Issue 10 of the report, online: Industry Canada <http://strategis.ic.gc.ca/SSG/ih01041e.html> (date accessed: 28 November 2000).

116 Canada, Information Highway Advisory Council Secretariat, *Building the Information Society: Moving Canada Into the 21st Century* (Ottawa: Minister of Supply and Services Canada, 1996) at 25, online: Industry Canada <http://strategis.ic.gc.ca/pics/ih/21st_e.pdf> (date accessed: 8 November 2000).

117 S.Q. 1993, c. 17, P-39.1, online: Les Publications du Québec <http://publicationsduquebec.gouv.qc.ca/documents/lr/P_39_1/P39_1_A.html> (date accessed: 15 March 2001). This legislation took effect 1 January 1994.

118 *Supra* note 3. The Model Code as it appears in Schedule 1 of the *Act* is reproduced in Appendix 3.

119 T. Scassa, "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation" (2001) 32:1 Ottawa L. Rev. 3 at 6.

120 G. Greenleaf, "Stopping surveillance: Beyond 'efficiency' and the OECD" (December 1996), online: Australasian Legal Information Institute <http://www2.austlii.edu.au/itlaw/articles/efficiency.html> (date accessed: 20 September 2000).

121 *Ibid.*

purposes by broadly defining those purposes from the outset. However, he concedes that regulations or laws focused on the efficiency principle are better than none at all.[122]

Incidentally, a recent Canadian study makes that very point.[123] From May to December 2000, of 259 web sites surveyed based in or targeting Canada, 41 percent of the sites had no privacy policy available online. When considering only the 194 sites of Canadian origin, half had no privacy policy.[124] Even those that did have policies often had ones that would be considered non-compliant with the *PIPA*. For example:

- 46 percent of the privacy policies did not reveal the purpose of the information collection;
- 57 percent of the policies provided no contact information; and
- 90 percent of the policies provided no information regarding updating personal information.[125]

The authors found that these and other lapses were more common in sites based in Canada or elsewhere that target this country than for those in the United States. One of the authors raises the possibility that the American sites may be more sensitive to privacy issues because of the self-regulatory push south of the border.[126] For instance, while 32 percent of the Canadian sites were found to collect substantial amounts of personal information despite having no privacy policy, this was only the case for 10 percent of sites from elsewhere. Whereas 63 percent of Canadian sites failed to provide contact information, only 33 percent of offshore sites did.[127] The study did find better privacy practices among Canadian web sites within regulated sectors of the economy such as banking and health care.[128] As the new privacy legislation begins to take hold, these figures should rise in all sectors. The amount of "surveillance" may not decrease, but one would expect it to at least be more open and fair.

However, this will not necessarily be the case according to the findings of a study contrasting privacy practices on American and European web sites.[129] Although Europe has tougher, more comprehensive data protection laws than the United States, it did not

---

122 *Ibid.*

123 M. Geist & G. Van Loon, "Canadian E-Commerce and Privacy Study 2000: A Failure to Communicate" (December 2000), online: University of Ottawa Faculty of Law <http://aix1.uottawa.ca/~geist/privacystudy.htm> (date accessed: 7 December 2000). As of early August 2001, the full study had not been released but the major findings were available at this URL.

124 *Ibid.*

125 *Ibid.*

126 M. Geist, "A troubling snapshot of e-privacy in Canada" *The Globe and Mail* (7 December 2000), online: Globetechnology.com <http://www.globetechnology.com/archive/20001207/TWGEIS.html> (date accessed: 30 June 2001).

127 *Supra* note 123.

128 *Supra* note 126.

129 K. Scribbins, "Privacy@net: An International Comparative Study of Consumer Privacy on the Internet (January 2001), online: Consumers International <http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf> (date accessed: 25 January 2001).

follow that the sites there were better at protecting consumers. In fact, sites in the United States "tended to set the standard for decent privacy policies."[130] These standard-bearers, while in the minority, were among the most popular on-line destinations, which may be evidence for the common assertion that good privacy policy is good business. On the other hand, it could also be that the more popular, and thus more profitable, sites can afford the time to engineer good policy or to hire the expertise to do so. Overall, the vast majority of the 751 sites surveyed on both sides of the Atlantic fell "woefully short" of internationally accepted data protection guidelines.[131] The overall message is of a failure of self-regulation in the United States and a lack of enforcement in Europe.

It will be interesting to see if the *PIPA* has had more success once it has been in place for a few years. At present, the *Act* applies only to the clients and the employees of the federally regulated private sector: for example, banking, telecommunications, transportation and broadcasting, and businesses that move data across provincial or international boundaries. In 2002 the *Act* will apply to the health care sector. In 2004 it will apply to provincially regulated sectors in any province that has not enacted its own substantially similar legislation. The European Union must now decide whether the *PIPA* conforms to the "adequate protection" provision of the EU *Directive*. If the answer is no, Canada might be expected to look to the American model and to try to enter into an agreement similar to Safe Harbor.[132] An opinion[133] issued by an EU advisory body on data protection and privacy advises the European Commission, among other things, that any adequacy finding for the *PIPA* should consider the timetable for implementing the *Act* and its limited scope;[134] that is, it applies only to commercial activity. It appears that a finding of adequacy is by no means guaranteed.

IV. TRUSTMARKS IN THE DATABASE NATION AND BEYOND

The United States Federal Trade Commission's early reluctance to recommend privacy legislation for the on-line world was underscored by demands for industry to act responsibly and to regulate itself. TRUSTe was the first organization to recognize the opportunity that had been created for an intermediary willing to verify and vouch for a web site's privacy practices. The independent, non-profit organization promotes itself as a cost-effective alternative to government oversight, which "would likely be more rigid,

---

130 *Ibid.* at 6.

131 *Ibid.* at 5.

132 However, the failure of many companies to register for that program in its first months of operation was raising questions about its effectiveness. Only 88 companies were on the Department of Commerce's Safe Harbor List, online: United States Department of Commerce <http://web.ita.doc.gov/safeharbor/SHList.nsf/WebPages/Safe+Harbor+List> (date accessed: 15 August 2001). See D. McCullagh, "Safe Harbor Is a Lonely Harbor" *Wired News* (5 January 2001), online: Wired News <http://www.wired.com/news/politics/0,1283,41004,00.html> (date accessed: 6 January 2001).

133 EU Article 29 — Data Protection Working Party, *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*, online: The European Union <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp39en.pdf> (dated accessed: 12 March 2001).

134 *Supra* note 129 at 7.

costly to implement, and difficult to repeal."[135] Officially launched in June 1997, TRUSTe is equal parts idealism and pragmatism. Its founding partners are two other non-profit organizations: The Electronic Frontier Foundation, which promotes privacy, free expression, and social responsibility in new media and CommerceNet, which works to promote and advance e-commerce.[136] The more that TRUSTe's work manages to overcome consumers' reluctance to shop online, the more CommerceNet has to gain through a broader market for its own services.

TRUSTe is easily the largest and best known privacy trustmark.[137] In November 2000 it boasted over 1,500 clients,[138] including Microsoft, America Online, RealNetworks, and Global TV's various regional sites.[139] Initially, the requirements necessary to be awarded a TRUSTe seal were minimal. Basically, the appearance of the company's trustmark certified little but the existence of a privacy policy, whatever its contents.[140] As of January 1, 2000, however, all licensees have been required to meet a higher standard. Clients' privacy policies must now address the four substantive FIPs: Notice, Choice, Access and Security. That being the case, TRUSTe permits licensees to display the organization's privacy seal as well as a "click to verify" seal that is displayed alongside the privacy policy. Consumers who click it are taken to a statement on TRUSTe's secure server that confirms that the endorsement is authentic.

TRUSTe undertakes to periodically seed licensed web sites with unique personal information in an effort to uncover any violations of the stated privacy policy.[141] It also conducts random checks of the site for compliance, and it acts on complaints from the on-line community.

---

135 TRUSTe, "Why is self-regulation so important?" (2000), online: TRUSTe <http://www.truste.org/about/truste/about_faqs.html#self> (date accessed: 11 November 2000).

136 *Ibid.*

137 BBBOnLine's Reliability Seal trustmark program had 9,518 members as of March 17, 2001, but its basic requirement is membership in the Better Business Bureau. Privacy issues are not addressed and there was a built-in customer base when the program began. BBBOnLine, online: BBBOnLine Homepage <www.bbbonline.com> (date accessed: 17 March 2001).

138 A complete list of TRUSTe participants can be found online: TRUSTe <http://www.truste.org/users/users_lookup.html>. The company officially claimed "nearly 2,000 certified Web sites" in its press releases in November 2000, but there was no counter on its site such as that found on BBBOnLine. Online: TRUSTe <http://www.truste.org/about/about_tips2000.html> (date accessed: 23 June 2001). Counting individual licensees, which is possible with WebTrust because there are so few, was not practical in this case.

139 See for instance Global Television, online: Global TV <http://atlantic.globaltv.com> (date accessed: 11 November, 2000).

140 Center for Democracy and Technology, "Behind the Numbers: Privacy Practices on the Web" (27 July 1999), online: Center for Democracy and Technology <http://www.cdt.org/privacy/990727privacy.shtml> (date accessed: 9 November 2000). See Section IV.A.

141 This process is not explained in depth on TRUSTe's web site, but e-mail correspondence from the company confirmed that they submit a unique identifier to the web site of a licensee and then wait to see if it is used in ways counter to stated policies. Since TRUSTe does not have access to the licensee's database, the only way that they know if information is being misused is if an unapproved offer or marketing is later aimed at that identity. This seems like an awkward test, since the information might be used inappropriately in less obvious ways. TRUSTe Business Development, "Re: Seeding Web Sites," e-mail to John MacDonnell (8 December 2000).

On November 1, 2000, TRUSTe began a new effort, the European Union Safe Harbor Privacy Seal program. Web sites that carry this new seal must comply with the US Department of Commerce's Safe Harbor Privacy Framework. TRUSTe also has a children's privacy seal program with conditions that coincide with the *Children's Online Privacy Protection Act of 1998.*

In March 1999 BBBOnLine, a subsidiary of the Council of Better Business Bureaus, began to compete with TRUSTe in the issuance of privacy seals. It had established itself in 1997 with a program to issue reliability seals for web sites operated by BBB members. This privacy seal program requires sites to display privacy policies addressing notice, choice, access, and security. In November 2000, 698 web sites were participating in the program,[142] including American Airlines, Nestle, and Eastman Kodak. BBBOnLine takes applications from outside the United States,[143] and it has entered a joint on-line privacy seal venture with a Japanese trustmark provider to automatically issue shared seals to each other's program participants.[144]

There are a growing number of entrants in the trustmark field,[145] but TRUSTe and BBBOnLine are the only ones with significant presence on the Web to date. CPA WebTrust (Chartered Public Accountant), which had only 29 clients[146] as of November 2000, is among the most prominent after the two market leaders. The American Institute of Chartered Public Accountants and the Canadian Institute of Chartered Accountants jointly developed WebTrust. This probably accounts for the presence of six Canadian sites in its short client roster. Among the more notable names are Bell Canada, Air Miles, and E*TRADE's American and Canadian operations.[147]

WebTrust explicitly contrasts itself with its two larger competitors. WebTrust points out that it acts to prevent privacy breaches through regular audits by a chartered public accountant of a site's "policies, procedures, disclosures, technology and

---

142 Current participants may be found at BBBOnLine, online: BBBOnLine Homepage <http://www.bbbonline.com.>.

143 No Canadian businesses were readily apparent in the BBBOnLine Privacy Program participant listings, which are displayed in such a way as to make it tedious to check. A company representative did not know of any offhand in an e-mail exchange.

144 H. Cherico, "New Online Privacy Protection Tool to Transcend Borders; BBBOnLine and Japanese Privacy Seal Program (JIPDEC) Announce Plans for Joint Online Privacy Seal Venture" (18 May 2000), online: <http://www.bbbonline.org/about/press/2000/051800.asp> (date accessed: 4 December 2000).

145 See, for instance, the PricewaterhouseCoopers BetterWeb program online: PricewaterhouseCoopers <http://www.pwcbetterweb.com>; Clicksure online: Clicksure <http://www.clicksure.com>; and for a sector specific program, the Entertainment Software Rating Board's privacy seal initiative online: ESRB <http://www.esrb.org/privacy.asp>.

146 For a current client list, see online: Verisign Inc. <http://www.verisign.com/webtrust/siteindex.html>. The number had risen to 31 clients in mid-March 2001. Confusingly, a second list with the same clients but fewer of them is maintained online: WebTrust <http://www.webtrust.org/abtseals.htm>. Only 24 clients were listed at this site in mid-March.

147 *Ibid.*

infrastructure."[148] WebTrust contends that BBBOnLine and TRUSTe rely on promises to respect privacy policies and that they only take action if those vows are broken. Another difference is that WebTrust has developed standards in addition to on-line privacy, including transactional integrity and security.[149]

Of the three trustmark providers, TRUSTe is most often the subject of criticism. This is not necessarily a reflection of its practices compared to its competitors. Rather, as a larger target, it simply draws more attention in all respects. In 1999, for example, the company came under fire because it failed to reprimand Microsoft or RealNetworks for gathering information on users via software.[150] TRUSTe responded that its seal covers activity on a web site, not the operation of software on an end-user's computer. Since then, it has taken steps to develop a software privacy seal.[151]

The fact that these three trustmark programs are not entirely similar, and are possibly complementary in some cases, is supported by the appearance of multiple marks on some sites. The American E*TRADE[152] site, for instance, at one time displayed the trustmarks of both TRUSTe and WebTrust. Another American financial site, E-LOAN.com,[153] boasted four privacy-related seals: TRUSTe, BBBOnLine, PricewaterhouseCoopers BetterWeb, and a second PricewaterhouseCoopers seal that links directly to an audit report of the site's privacy practices. This last seal is part of an emerging trend in the industry for more comprehensive audits of privacy practices performed by one of the "big five" accounting firms.[154] Unlike TRUSTe's privacy audits from afar, these audits involve office visits. In the case of E-LOAN, for example, three employees of the auditor were on site for three weeks.[155] These "audit seals" are more an adjunct to the other programs though, as indicated by the existence of PricewaterhouseCoopers own BetterWeb trustmark. WebTrust could be viewed as a hybrid of this approach and of the less rigorous schemes of BBBOnLine and TRUSTe.

---

148 WebTrust, Press Release "WebTrust Program for On-Line Privacy Continues to Help American Companies Comply With E.U. Safe Harbor Privacy Provisions" (6 November 2000), online: WebTrust <http://www.webtrust.org/abtpress.htm#nov600.htm> (date accessed: 14 January 2001).

149 *Ibid.*

150 M. Kessler, "Online privacy still a hot-button issue: seal plans have advocates, critics" *USA Today* (24 July 2000), online: USA Today <http://www.usatoday.com/life/cyber/tech/cti269.htm> (date accessed: 16 November 2000).

151 See the response to a question from a forum participant in Vienna, VA, in D. Steer, "Protecting Your Privacy with Dave Steer of TRUSTe." *Washington Post* (1 March 2001), online: WashingtonPost .com <http://discuss.washingtonpost.com/wp-srv/zforum/00/singletary0719.htm> (date accessed: 1 March 2001).

152 Etrade.com, online: Etrade.com Homepage <http://www.Etrade.com> Note, since the writing of this article, E*TRADE no longer has any trustmarks visible on the site (date accessed: 15 July 2001).

153 E-LOAN.com, online: E-LOAN.com Homepage <http://www.E-LOAN.com> Note, since the writing of this article, E-LOAN now displays the PricewaterhouseCoopers BetterWeb mark and the PricewaterhouseCoopers privacy seal (date accessed: 15 July 2001).

154 B. Tedeschi, "Sellers Hire Auditors to Verify Privacy Policies and Increase Trust" *The New York Times* (18 September 2000), online: The New York Times <http://www.nytimes.com/2000/09/18/technology/18ECOMMERCE.html> (date accessed: 18 September 2000).

155 *Ibid.*

In September 1999 the participants of the 21st Conference of International Data Protection Commissioners decided that trustmarks, or web privacy seals as they prefer to call them, had developed a sufficient presence in the on-line world to be worthy of study.[156] The idea was that objective standards should be applied in order to measure the usefulness of these increasingly common tools. To that end, the Information and Privacy Commissioner of Ontario and the Federal Privacy Commissioner of Australia undertook to study BBBOnLine, TRUSTe, and WebTrust.[157] The researchers broke the on-line seal programs into three key components:

- sufficient privacy principles to which participating Web sites must adhere;
- an effective method for resolving disputes between consumers and Web sites; and
- a robust mechanism for ensuring that sealed Web sites comply with the standards set.[158]

The next step was to devise separate methodologies for evaluating each component: privacy protection, dispute resolution, and compliance. For the purposes of the current article, the data commissioners' method of assessing the privacy protection component has been adopted and adapted. Before delving into those results it is instructive to review the privacy findings of the earlier study. In that study the researchers read all of the applicable material that was publicly available for viewing from the web sites of the three trustmark programs in November 1999. They then compared those documents to the 16 criteria that they had developed by further breaking down the eight principles of the OECD *Guidelines*. Each principle was assigned one point, which was then divided equally among the criteria with which it was associated.[159]

For example, only one criterion fell under the Security Safeguards principle, so it was valued at one point.[160] On the other hand, the Individual Participation principle was divided into four criteria, each worth 0.25 of a point.[161] In the end, a trustmark program that met all 16 criteria would garner eight points. The researchers acknowledged the following limitations to this methodology:

- A quantitative assessment does not necessarily capture the full scope of a seal program. It does not cover items such as efforts at consumer and business education; and
- A failure to refer to a particular criterion present in the OECD *Guidelines* could not validly lead to the conclusion that the program would endorse or permit policies and practices counter to that condition.[162]

---

156 Cavoukian & Crompton, *supra* note 13.
157 *Ibid.* at 3.
158 *Ibid.* at 6.
159 *Ibid.* at 8, 9.
160 *Ibid.* at 8.
161 *Ibid.* at 9.
162 *Ibid.* at 10.

Consequently, the final value assigned to each trustmark was not exactly a score that would afford one program bragging rights over another. Rather, it was a diagnostic tool that could be used to see where there were possible gaps between the policies of the three programs and the voluntary *Guidelines*. The deficits pointed out in the analysis were consistent. None of the programs fully met the *Guidelines* in the opinion of the reviewers, and each one failed to have a requirement to:

- Limit collection to fair and lawful means;
- Ensure that personal data is relevant to its intended purposes;
- Provide information to the data subject in a "reasonable time and manner," without excessive charge, and "in an intelligible form"; and
- Provide reasons for any denial of access to personal information about the data subject.[163]

An aspect of the study that was as important as the evaluation itself was an intent to begin a dialogue between the data commissioners and the seal providers. As such, each one was provided with the preliminary results of the study for consideration and response. For instance, BBBOnLine and TRUSTe took issue, among other things, with the researchers' contention that they had failed to have a requirement limiting data collection to lawful and fair means. The former insisted that a web site collecting data in violation of the law could not bear its privacy seal because it is a program requirement that participants not be engaged in illegal activity. Surely, though, collecting data by fair means is a more stringent test than merely lawful means. There is much in the world that is lawful, yet unfair.

For its part, WebTrust undertook to address the concerns raised by the comparison of its program with the OECD *Guidelines*. The other programs did not make such a broad commitment, but agreed to continue working with the data protection commissioners. They are constantly adapting to change in the on-line environment as it is. This is reflected by the fact that documents central to all three of these programs were modified in the year between November 1999, when the data protection commissioners studied them, and November 2000, when they were examined for the purposes of this article. By then, BBBOnLine claimed that its program incorporated all of the requirements of the EU *Directive*,[164] TRUSTe was offering its EU Safe Harbor Privacy Seal,[165] and WebTrust

---

163 *Ibid.* at 11.

164 *European Union Data Directive Compliance*, online: BBBOnLine <http://www.bbbonline.com/intl/index.asp> (date accessed: 15 November 2000).

165 D. Steer, "TRUSTe Unveils European Union Safe Harbor Privacy Seal Program" (1 November 2000), online: TRUSTe <http://www.truste.com/about/about_eu.html> (date accessed: 2 November 2000). TRUSTe was the first organization to enter the safe harbour according to the US Department of Commerce Safe Harbor List, online: United States Department of Commerce <http://web.ita.doc.gov/safeharbor/SHList.nsf/WebPages/Safe+Harbor+List> (date accessed: 2 November 2000).

declared that Version 3 of its privacy benchmark "substantively" met the privacy standards of the European Union and Canada.[166]

A. THE *PIPA* PARED DOWN

Because the European and Canadian legislation are closely linked to the earlier work of the OECD, the latest claims of the trustmark providers could not be valid without better compliance with the *Guidelines*. That made the choice of methodology for the current review of the programs a simple one. The procedures of the data commissioners' study were adapted for use with the criteria found within Canada's new federal legislation. Unlike the eight pithy *Guidelines*, the CSA Model Code as presented in Schedule 1 of the *Act* is an almost conversational document that introduces one of its ten principles and then elaborates on it, sometimes at length. In addition, Part 1 of the *PIPA* has to be closely read for any clauses that affect the code.[167] In the end, the *Act* was reduced to 31 criteria to be compared with the trustmark programs. It is meant to be a representative list rather than an exhaustive one. The 31 criteria and the principles from which they arise are listed in the following table. Unlike the previous study's assignment of a single point to each principle, which was then divided among the associated criteria, each criterion in this case is assigned one point. However, there is no sense that each criterion is equally valuable; this is simply a way to develop a rough guide as to how closely each of the trustmarks comes to meeting all of the criteria. It is not so much a grade as it is a roll call. The presence of a criterion merits a point; the absence, no points. In cases where there seems to be partial fulfillment, a half point is awarded.

TABLE I: *PERSONAL INFORMATION PROTECTION ACT* — EVALUATION CRITERIA[168]

ACCOUNTABILITY PRINCIPLE: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
1. Data controller(s) accountable for compliance with principles
2. Data controller(s) identity available on request
3. Contractual or other means used to assure comparable protection of information transferred to third parties for processing
IDENTIFYING PURPOSES PRINCIPLE: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
4. Specify purposes to data subject at or before time of collection

166 "Global Reach Sets an International Standard" *Overview of the WebTrust 3.0 Program*, online: WebTrust <http://www.webtrust.org/onlnover.htm> (date accessed: 30 November 2000).

167 Schedule 1 of the *Act* in Appendix 3 has notes added to indicate where it is modified by Part 1 of the *Personal Information Protection and Electronic Documents Act*.

168 These principles are from Schedule 1 of the *PIPA*, *supra* note 3. Criteria 1-31 extend with the author's own analysis of those principles.

CONSENT PRINCIPLE: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
5. Knowledge and consent of data subject 6. Product or service cannot be denied if data subject refuses to divulge information beyond that required for specified, legitimate purpose 7. Data subject may withdraw consent
LIMITING COLLECTION PRINCIPLE: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
8. Data collection limited to that necessary for identified purposes 9. Data collection only by lawful and fair means
LIMITING USE, DISCLOSURE, AND RETENTION PRINCIPLE: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
10. Use and disclose in accordance with specified purposes 11. Except with data subject consent or by authority of law 12. Data retained only as long as necessary for specified purposes 13. New uses of personal information shall be documented
ACCURACY PRINCIPLE: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
14. Accurate, complete and up-to-date as necessary for specified purposes
SAFEGUARDS PRINCIPLE: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
15. Appropriate security safeguards
OPENNESS PRINCIPLE: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
16. Ready access for data subject to policies and practices 17. Policies and practices available in generally understandable form 18. Ready access to description of type of personal information held, including general account of its use 19. Ready access to description of what personal information made available to related organizations
INDIVIDUAL ACCESS PRINCIPLE: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
20. Data subject informed of existence, use, and disclosure of personal information 21. Data subject can access personal information 22. Personally identifying information disclosed to gain access to information shall be used for no other purpose 23. Data communicated within 30 days and at a minimal or no cost to the individual 24. Requested information must be in a form that is generally understandable

25.	Reasons for denying access set out along with any available recourse
26.	Ability to challenge and amend
27.	Where appropriate, amended information passed on to third parties with access
28.	Substance of unresolved challenges to information shall be recorded
29.	Where appropriate, existence of unresolved challenges transmitted to third parties with access
CHALLENGING COMPLIANCE PRINCIPLE: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.	
30.	Data subject can challenge compliance with principles
31.	Justified complaints addressed by appropriate measures, including, if necessary, amending policies and practices

Of the 31 *PIPA* criteria listed above, 14 are either stronger than any similar criteria in the OECD *Guidelines* or are not contemplated. This is not surprising when one considers that the CSA Model Code was developed more than a decade after the completion of the OECD's efforts. The authors of the *Guidelines* stated that they should be regarded as "minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties."[169]

Of the four criteria that Cavoukian and Crompton[170] found to be important obstacles to the compliance of the trustmark providers with the *Guidelines*, only one makes no direct appearance in Schedule 1 of the *Act*. The missing criterion is the requirement that personal data be relevant to the purposes for which they are to be used. Instead, the Limiting Collection principle has the more stringent criterion that the collection of personal information be limited to that which is necessary for the purposes of the organization. Although "necessary" and "relevant" are not synonymous, their effect in these clauses is roughly similar. Notably, all three seal providers refrain from using either word in their criteria that fall under the Limiting Collection principle. The authors of the earlier web seal review conclude: "Our most significant concern related to the lack of a requirement on seal participants to restrict their use of personal information to that which was *relevant* and *necessary* for the purposes for which the data was collected."[171] The authors believe that determining relevancy is a critical aspect of limiting data collection and that the burden of this determination should be placed on the collecting organization rather than on consumers. "Ideally, if a piece of personal information was not absolutely required to complete a transaction, it should not be used."[172]

Overall, the *Act* tends to strengthen and extend the principles found in the *Guidelines*, sometimes in subtle ways. Where the OECD seeks "knowledge or consent" of the data subject before collecting information,[173] the Model Code contemplates the stronger "knowledge *and* consent."[174] The Consent principle also increases protections to the

---

169 *Guidelines*, *supra* note 15 at Part 1, General, Scope of Guidelines, 6.

170 *Supra* note 13.

171 *Ibid.* at 23 [emphasis added].

172 *Ibid.* at 13. Curiously, the quoted sentence ends with "it should not be *used*," rather than *collected*.

173 *Supra* note 15 at 3.

174 Schedule 1, *supra* note 3 at 4.3 Principle 3.

individual with two additional criteria: one regards withdrawal of consent[175] and the other an organization's obligation to serve customers who refuse to divulge information as long as the requested information is not required for a legitimate purpose.[176]

The appearance of "should" several times within Schedule 1 of the *Act* appears to weaken certain aspects of the legislation, or it introduces an unhelpful degree of uncertainty. In Part 1, the *PIPA* spells out the legal meaning of *should* as far as the *Act* is concerned: "The word 'should,' when used in Schedule 1, indicates a recommendation and does not impose an obligation."[177] What is one to make of the following apparent conflicts within the Identifying Purposes principle and the Accuracy principle?[178]

> 4.2 The purposes for which personal information is collected *shall* be identified by the organization at or before the time the information is collected.[179]
>
> 4.2.3 The identified purposes *should* be specified at or before the time of collection to the individual from whom the personal information is collected.[180]
>
> 4.6 Personal information *shall* be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.[181]
>
> 4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, *should* generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.[182]

For the purposes of this article, it is assumed that the word *shall* in 4.2 and 4.6 overrides the use of *should* in 4.2.3 and 4.6.3, respectively. Other places in which *should* appears in Schedule 1, thus turning what would be a good policy requirement into a recommendation, include:

> 4.5.2 Organizations *should* develop guidelines and implement procedures with respect to the retention of personal information. These guidelines *should* include minimum and maximum retention periods.[183]
>
> 4.5.3 Personal information that is no longer required to fulfil the identified purposes *should* be destroyed, erased, or made anonymous.[184]

---

175 *Ibid.* at 16.
176 *Ibid.* at 14.
177 *Supra* note 8 at Part I. 5. (2).
178 Italics added to demonstrate the conflicts between criterion using *shall* and those using *should.*
179 Model Code, *supra* note 3 at 12.
180 *Ibid.* at 13.
181 *Ibid.* at 17, 18.
182 *Ibid.* at 18.
183 *Ibid.* at 17.
184 *Ibid.*

4.10.2 The complaint procedures *should* be easily accessible and easy to use.[185]

To further add to the confusion, in Part 1, s. 11.(1), the *Act* declares that "[a]n individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1."[186] Despite the fact that certain aspects of the schedule are to be taken as recommendations rather than obligations, individuals may still lodge a complaint when they have not been followed. This bears out the criticism that adopting a model code as law is not necessarily as viable an option as adapting a model code for the purposes of new legislation.[187] It may also help to avoid the contortions required in the *Act* to ensure data subjects are given reasons for any denial of access to personal information held about them. In the Individual Access principle, Schedule 1 stipulates that "[t]he reasons for denying access *should* be provided to the individual upon request."[188] To prevent this important concept from being merely a recommendation rather than an obligation, the *Act* specifies, in Part 1 at 8.(7), that an organization rejecting a request for information "shall inform the individual in writing of the refusal, setting out the reasons and any recourse they may have under this Part."[189] Obviously, the legislation has to be carefully scanned for additions or deletions to the Model Code that it has embraced. Perhaps the most significant clause in the *PIPA* occurs in Part 1 at 5.(3): "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[190] This clause is not a criterion taken from the Model Code, but it could well be the subject of debate in the office of the privacy commissioner or in the courts in the near future.

The criteria chosen for this analysis certainly do not tell the entire story of the *PIPA*. With that in mind, the results of the analysis are highlighted below. Appendices 4, 5, and 6 contain tables that display trustmark criteria deemed comparable to the *PIPA* criteria. The comparison uses only material publicly available from the seal providers' web sites in November 2000. Where uncertainty exists, the documents have been interpreted to give the companies the benefit of the doubt.

B. FALLING SHORT OF THE MARK

None of the trustmark programs examined appear to have explicit criteria in place that would allow them to claim full compliance with the law in the *Personal Information*

---

185 *Ibid.* at 22.

186 *Supra* note 8.

187 Ontario's Ministry of Consumer and Commercial Relations raises this point in a recent paper: Ontario, Ministry of Consumer and Commercial Relations, *A Consultation Paper: Proposed Ontario Privacy Act* (Ontario: July 2000) at 4, online: Ministry of Consumer and Business Services <http://www.ccr.gov.on.ca/pdf/PrivacyPaper.pdf> (date accessed: 1 December 2000). "[A]lthough the CSA Standard is well suited to be applied as a voluntary code, not all of its elements may be well suited for legislation. Therefore, Ontario is considering each element of the CSA Standard and whether it would make an appropriate statutory requirement."

188 Schedule 1, *supra* note 3 at 20.

189 *Supra* note 8.

190 *Ibid.*

Protection Act. As in the earlier study, they tend to share common deficits. In particular, they fail to fully address the following evaluation criteria set out previously in Table I:

Individual Access Principle

1) Personally identifying information disclosed to gain access to information shall be used for no other purpose;
2) Where appropriate, amended information passed on to third parties with access;
3) Substance of unresolved challenges to information shall be recorded;
4) Where appropriate, existence of unresolved challenges transmitted to third parties with access;

Limiting Use, Disclosure, and Retention Principle

5) Data retained only as long as necessary for specified purposes;

Challenging Compliance Principle

6) Justified complaints addressed by appropriate measures, including, if necessary, amending policies and practices; and

Limiting Collection Principle

7) Data collection only by lawful and fair means.

Of the seven shared shortfalls identified, the first six go beyond anything that appears in the *Guidelines*. The last common shortfall is familiar from the first study. As a whole, they offer some important safeguards for personal identifying information. The first prevents an individual who is curious to discover exactly what information about them is held from inadvertently supplying yet more grist for the databank mills while proving their identity. The second ensures that once information is amended, it is passed along to third parties who may be using the original, unamended data. It does not do the consumer any good to correct faulty information at one source, only to have it appear unaltered at another. The third criterion gives the consumer the opportunity to tell his or her side of the story should the organization holding the data refuse to amend the personal identifying information that it holds. The fourth ensures that interested third parties know about the unresolved challenge. Number five is a strong deterrent against what could be called *usage creep*, the temptation to find other uses for data that has already been acquired. Number six seeks to prevent a cycle of repeated transgressions, with a specific assurance that valid complaints will lead to action, which may include changes to inadequate policies or practices.

The final criterion has already been mentioned in relation to the OECD *Guidelines* study, and the trustmark providers still fall afoul of it a year after it was identified by those researchers. No one makes an explicit demand that data be collected only by fair

means. Perhaps BBBOnLine's argument,[191] that something that is unfair would naturally be unlawful, has more resonance if the services of the trustmark providers are restricted to the United States. After all, the *Federal Trade Commission Act*[192] empowers that agency to prevent unfair or deceptive acts or practices, in or affecting commerce. However, if the trustmarks are seeking to do business beyond American borders, it is logical for this restriction to be specified. Indeed, even in the home base for these trustmarks, an unequivocal commitment to fairness would broaden their claims to be defenders of privacy.

To some degree, all three trustmarks also fail to explicitly deal with the criterion that was phrased in the *Guidelines* study[193] as a requirement to give "the data subject the right to have data related to him communicated in a reasonable time and manner, without excessive costs, and in an intelligible form."[194] In the present analysis, that criterion was split into two:

1) Data communicated within thirty days and at a minimal or no cost to the individual; and
2) Requested information must be in a form that is generally understandable.

WebTrust does not specify either of these criterion. BBBOnLine also fails to address the second criterion, but partially deals with the first by specifying that a cost over $15 US would be considered to be unreasonable. Timeliness is not mentioned. TRUSTe is the only one to clearly meet the second criterion: "The Personally Identifiable Information must be provided to users in a readily intelligible form." This would appear to be a major oversight on the part of TRUSTe's competitors. Regardless of how timely or inexpensively the information is acquired, it does not matter if it is in an unintelligible form. That said, TRUSTe fails on the first criterion. It specifies a thirty-day time limit in which to provide the requested information, but does not mention the cost. Overall, there is a large gap between what the trustmark providers seek to ensure in terms of individual access and what is expected under the terms of the *PIPA*. Issues and deficits that are not common to BBBOnLine, WebTrust, and TRUSTe are considered below for each program individually.

1. BBBONLINE

As with the other two programs, any document publicly available on the BBBOnLine web site that appeared to be related to its privacy seal was studied for indications that the program had standards equivalent to those in the *PIPA*. The documents actually quoted for the comparison are: the BBBOnLine Privacy Program Assessment Questionnaire,[195]

---

191 See Cavoukian & Crompton, *supra* note 13 at 12.

192 15 U.S.C. § 41 (1994), online: United States Department of Health and Human Services: Food and Drug Administration <http://www.fda.gov/opacom/laws/ftca.htm> (date accessed: 13 March 2001).

193 *Supra* note 13.

194 *Ibid.* at 11.

195 Online: BBBOnLine <http://www.bbbonline.com/privacy/assess.pdf> (date accessed: 14 November 2000).

the BBBOnLine Privacy Program Assessment Questionnaire — Help Document,[196] BBBOnLine Privacy Program Participation Agreement,[197] and General Privacy Seal Program Requirements.[198] While examining these documents, it became apparent that BBBOnLine has its own notice problems. The last document had been known as Privacy Program Eligibility Requirements when downloaded as a Portable Document Format ("PDF") file on November 14, 2000, but eight days later it had a new name and some new content. This change was made without any notification on the web site, and no "last updated" notice appeared on the document itself. It would be very easy for someone to browse the site on different occasions but be unaware that any program changes had been made, which seems unnecessarily careless for a policy driven organization. Ironically, one of the *PIPA* criteria that BBBOnLine fails to address, while the others do, is the requirement that "new uses of personal information shall be documented."[199] Basically, this is the same problem; a change can be made, and no one is the wiser.

If interpreted broadly, the stipulation in BBBOnLine's General Privacy Seal Requirements that "[o]rganizations must be engaged in activity that is legal"[200] could be read as a catch-all that will fill in any gaps between what the program explicitly requires and what is sought by the *PIPA*. After all, when applied in Canada this clause could be seen as an exhortation to abide by the letter of the law. However, the subclauses[201] make it appear that this particular program requirement is more about protecting the reputation of BBBOnLine than protecting consumers. This is not the case for a series of clauses that are part of the WebTrust program, which will be explored at greater length below.

2. TRUSTe

Documents quoted for the analysis of the TRUSTe program are: the TRUSTe License Agreement Version 6,[202] the TRUSTe Site Coordinators Guide,[203] the TRUSTe

---

196 Online: BBBOnLine <http://www.bbbonline.com/privacy/AssessH.pdf> (date accessed: 14 November 2000).

197 Online: BBBOnLine <http://www.bbbonline.com/privacy/license.pdf> (date accessed: 14 November 2000).

198 Online: BBBOnLine <http://www.bbbonline.com/privacy/threshold.pdf> (date accessed: 23 November 2000).

199 See Table 1, *supra* note 168 at criterion 13.

200 BBBOnLine, *General Privacy Seal Program Requirements*, *supra* note 198 at 1, clause 4 under Threshold Requirements, Eligible Organizations.

201 *Ibid.* Organizations "may not:
a) display content of such as obscene, defamatory, or hateful nature that it reflects unfavorably on the BBBOnLine Privacy Seal, or
b) engage in any activity that lessens the BBBOnLine Privacy Program's ability to promote trust and confidence on the Internet."

202 Online: TRUSTe <http://www.ftc.gov.os/2000/09/trustelicenseagreement.pdf> (date accessed: 14 November 2000).

203 Online: TRUSTe <http://www.truste.com/webpublishers/truste_scg.doc> (date accessed: 14 November 2000).

Program Principles,[204] and the Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0.[205]

The deficits found in the TRUSTe program that are not common to its competitors are rather curious omissions. First, there is the absence of any requirement for contractual or other means to assure comparable protection of information transferred to third parties for processing. It would do little good to promise consumers lofty privacy standards and then forward their data elsewhere to be processed in an environment that does not adhere to them. The second deficit is a hold-over from the Cavoukian and Crompton study.[206] Not only do TRUSTe's documents fail to mention an obligation for data collectors to use fair means, but there is also no requirement to adhere to lawful means. It is worth repeating that the absence of a standard cannot be construed as the encouragement of its opposite, but expressing an obligation to abide by the law would appear to be a reasonable step. Responding to this criticism when the authors of the previous study raised it, the director of compliance and policy for TRUSTe respectfully disagreed.[207] The director indicated that the program's self-assessment sheet, which licensees must complete and sign, provides an overview of data practices and policies that can be checked by the seal provider for illegal or unfair activity. This self-assessment sheet was not publicly available at the time of the previous study, so Cavoukian and Crompton did not review it. The sheet has been consulted for this analysis but the outcome is the same. TRUSTe is awarded zero points for this category, despite the detail that the sheet requires, because the word *lawful* casts a wide net that may catch activity not contemplated within the particulars of the self-assessment.

3. WEBTRUST

WebTrust distinguished itself among the three programs by having all of its relevant information available in a single document: WebTrust Program for Online Privacy Version 3.0.[208] But WebTrust's policies also had a very peculiar omission. The criterion under the Openness principle that policies and practices be made available in a generally understandable form is not addressed. However, three closely related criteria under the WebTrust banner could fill any gaps left by the lack of specific criteria. They are:

> A.6. The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.[209]

---

204 Online: TRUSTe <http://www.truste.com/webpublishers/pub_principles.html> (date accessed: 14 November 2000).

205 Online: TRUSTe <http://www.truste.org/webpublishers/harbor-addendum.doc> (date accessed: 24 June 2001).

206 *Supra* note 13.

207 *Ibid.* at 18.

208 Online: American Institute of Certified Public Accountants <http://ftp.aicpa.org/public/download/webtrust/nov28privacyfinal.doc> (date accessed: 8 December 2000) [hereinafter "WebTrust Program"]. Authorship is credited to the American Institute of Certified Public Accountants, Inc. ("AICPA") and Canadian Institute of Chartered Accountants ("CICA").

209 *Ibid.* at 24.

B.5. The entity's privacy and related security policies are consistent with disclosed privacy practices and applicable laws and regulations.[210]

D.2. The entity has procedures in place to keep its disclosed privacy and related security policies current with laws and regulations and to monitor adherence to its current privacy and security policy practices.[211]

Unlike BBBOnLine, these criteria appear to be expressly written in order to take into account legislation that goes beyond what is contemplated in WebTrust. This undoubtedly reflects that the program has greater international aspirations than do its two competitors. It would be nearly impossible to develop a program that explicitly details every policy that may be encountered in a country in which WebTrust is offered. Rather than attempt this, these clauses defer to the local chartered accountant or equivalent to ensure compliance with local regulations. Thus a web site that falls under Canadian jurisdiction and bears the WebTrust privacy seal would likely meet all of the *PIPA* criteria. However, a site falling under a non-Canadian jurisdiction, yet targeted at Canadians, could bear the same seal but operate under very different rules. In the borderless context of the Internet, this situation could be problematic for anyone who came to rely on the WebTrust assurance initially and was not aware of its implications when dealing with an offshore retailer that bore the same seal.

C. SURPASSING THE MARK

The three major privacy seal providers all come out wanting in an analysis of whether they explicitly meet the standards outlined in the *PIPA*. As discussed, especially where WebTrust is concerned, this does not necessarily mean that the program would not live up to the *Act* if applied as presented in its principles. As well, it has to be considered whether merely meeting the obligations of the *Act* should be enough to recommend a seal that oversees privacy in the on-line environment. After all, despite its genesis in legislation intended to support and promote electronic commerce, the *PIPA* applies to personal information whether it has been collected wholly online or entirely offline, which is as it should be. The rise of e-commerce has put abuses of personal information in the spotlight and has illuminated data protection practices in all spheres. However, the on-line world has its own particular perils that should be addressed by a privacy seal which, ironically, are not addressed by Canada's new federal legislation. It is instructive to take a second look at BBBOnLine, TRUSTe, and WebTrust with an eye to their advantages rather than their shortfalls. Some of those advantages would be useful in any context, others solely online.

The survey begins with some criteria that would not be out of place in the *PIPA* itself. BBBOnLine, for instance, requires that "[i]f information collected online is combined with data obtained from outside parties for purposes of an organization's marketing, the *privacy*

[210] *Ibid.* at 28.
[211] *Ibid.* at 36.

notice discloses this fact."[212] TRUSTe has a similar guideline that is broader because it does not restrict the need to disclose to occasions in which marketing is the aim. The Supplementation of Information policy reads:

> If the site is supplementing the information it receives directly from the users with information from any third party, then this must be disclosed as well. For example, if the site is only collecting names and email addresses via the web site, but is enhancing that information with additional information such as the preferences of those users from a third party, then the site must state this practice in the privacy statement. If your company compares lists in order to duplicate the data, then this should be included in your privacy statement as well.[213]

This important concept is not addressed in the *Act* or the OECD *Guidelines*. Clearly, it is as important to have notification of when personal information is being collected about an individual from third parties as it is to know when personal information is being distributed. Otherwise an organization could surreptitiously build an elaborate profile of any individual while seemingly collecting only minimal information.

BBBOnLine and TRUSTe also deal with another concept that should be considered in all data protection regimes — what they respectively call *prospect information* and *third party personally identifiable information*. In both cases the organization is referring to personally identifiable information that has been submitted by someone other than the individual to whom it directly relates. A common example would be an instance where someone buys a gift to be shipped directly to the recipient. The business gains access to a name and address, although the individual concerned had no knowledge of the transaction and no opportunity to consent to it. Both privacy seal providers restrict the uses of this prospect information and require program participants to give individuals the opportunity to opt in or opt out of any marketing targeted at them.[214]

When it comes to sensitive information, two of the seal providers deal with the issue in greater detail than does the *PIPA*. The subject is touched upon under the Consent and Safeguards principles of the CSA Model Code,[215] but not much guidance is offered. At clause 4.3.4, medical records and income records are put forth as examples of information "almost always" considered sensitive. However, what is sensitive is not defined any further, other than to note that "any information can be sensitive, depending on the context."[216] This vagueness is another example of drafting that, while fine for a model code, leaves something to be desired when it becomes legislation. It offers little guidance to an organization faced with the recommendation at clause 4.7.2 that "[m]ore sensitive

---

212 BBBOnLine, *General Privacy Seal Program Requirements*, *supra* note 198 at 3, clause 16 under Privacy Notice Requirements, Privacy Notice Content [emphasis in original].

213 TRUSTe, *TRUSTe Site Coordinator's Guide*, *supra* note 203 at 5, clause 3.1.5.

214 For TRUSTe, see 3.B.viii. Limit on Use of Third Party Personally Identifiable Information at 6 of Schedule A: Program Requirements in *TRUSTe License Agreement Version 6*, *supra* note 202. For BBBOnLine, see clause 2 under the heading Sharing of Information and under the heading Choice and Consent, both at 4 of *General Privacy Seal Program Requirements*, *supra* note 198.

215 *Supra* note 3.

216 *Ibid.* at 15.

information should be safeguarded by a higher level of protection."[217] In contrast, BBBOnLine divides sensitive information into two categories:

> 60. Type I Sensitive Information
>
> Type I sensitive information includes financial transaction data, such as credit card numbers, debit card numbers, check numbers, or bank account numbers. Type I sensitive data also includes social security numbers and health care information. Where Type I sensitive information is collected, the BBB*OnLine* requirement is that it be encrypted whenever it is transmitted or received online.
>
> 61. Type II Sensitive Information
>
> Type II sensitive information includes health care information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information specifying the sex life of an individual, or any other type of information that an individual identifies as sensitive. Where Type II sensitive information is collected, the BBB*OnLine* Privacy requirement is that such information may only be shared with outside parties or corporate affiliates with different privacy notices when the subject of that information expressly or affirmatively opts-in to that sharing (with certain *exceptions*). Please note that of the Type II categories, only health care information (which is also a Type I form of sensitive information) need be encrypted whenever it is transmitted or received online.[218]

WebTrust also is obviously influenced by the European model and is more exact when defining sensitive information. It is described as "personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offences or criminal convictions."[219]

All of the seal providers deal with the privacy of children's personal information. They are obligated to do so because of the existence in the United States of the *Children's Online Privacy Protection Act of 1998*,[220] but it appears to be an unfortunate omission from Canadian legislation.[221]

Following are some of the criteria provided by the seal providers that are relevant in an on-line context. BBBOnLine requires organizations to explain in their privacy notice if they link "*passive or behavioural information* (like cookies or purchase histories) with names or similarly specific identifiers."[222] Likewise, WebTrust requires that an on-line site using cookies, web bugs, or middleware to track customers disclose this fact.[223] As

---

217 *Ibid.* at 19.

218 BBBOnLine, *The BBBOnLine Privacy Program Assessment Questionnaire — Help Document*, *supra* note 196 at 13 [emphasis in original].

219 WebTrust Program, *supra* note 208 at 7.

220 *Supra* note 94.

221 Only a glancing reference to children is made in the *PIPA*. *Supra* note 8, at clause 4.3.6 of Schedule 1, it says, "Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney.)"

222 BBBOnLine, *General Privacy Seal Program Requirements*, *supra* note 198 at 3, clause 7 [emphasis in original].

223 WebTrust Program, note 208 at 23, clause A.2.

well, permission must be obtained before altering or copying information on a customer's computer or storing files there.[224] TRUSTe has the weakest policy addressing this issue because it is restricted to cookies, thus leaving the use of web bugs or middleware unaccounted for, and it is a recommendation rather than a requirement: "If the website stores information gathered through cookies in order to create a profile of the user, this should be disclosed to the user."[225]

Another aspect of the on-line experience addressed by all three of the privacy seal providers is the fact that visitors to a web site cannot always tell who is collecting information, or even when they have moved from one site to another with different policies in effect. WebTrust addresses this problem by requiring that "[t]he entity clearly discloses to the site's visitors when they have left the site covered by the entity's privacy policy."[226] However, this disclosure does not address situations in which multiple organizations are able to access information from a single site. TRUSTe addresses this by requiring that "[t]he Privacy Statement must identify anyone who collects or maintains personal information from or about the users of the Site, or has an interest in the information collected, or on whose behalf such information is collected or maintained."[227] This would seem to include advertisers, although neither TRUSTe nor BBBOnLine in its very similar policy[228] make this explicit.

A final example of a requirement present in a privacy seal program that would be worth repeating elsewhere is BBBOnLine's stipulation that any geographic limitations to a site's privacy notice should be explained. This requirement is particularly important in the on-line context, where the illusion of melting borders becomes less real each day as laws begin to replace anarchy on the cyberspace frontier.[229] In its Privacy Notice Content requirements, BBBOnLine states:

> If the organization limits the promises made in the privacy notice to *residents of one or more specific countries*, the site or service posts a statement (separate from the privacy notice) on the homepage, in each area where information is collected, and in each area where an email address is held out for the organization that states that the site or service is only for residents of those specific countries. In addition, the privacy notice must also disclose the limitation of the site or service to residents of those specific countries.[230]

---

224 *Ibid.* at 35, clause C.13.

225 TRUSTe, *TRUSTe Site Coordinator's Guide*, *supra* note 203 at 8, clause 4.6.

226 WebTrust Program, *supra* note 208 at 25, clause A.8.

227 TRUSTe, *TRUSTe License Agreement Version 6*, *supra* note 202 at 3, clause 2.F.ii.

228 BBBOnLine, *General Privacy Seal Program Requirements*, *supra* note 198 at 3, clause 17.

229 For an examination of the increasing pressure to erect virtual borders on the Web, see J.D. Glater, "Hemming in the World Wide Web" *The New York Times* (7 January 2001), online: The New York Times <http://www.nytimes.com/2001/01/07/weekinreview/07GLAT.html?pagewanted=all> (date accessed: 8 January 2001); and L. Guernsey, "Welcome to the World Wide Web. Passport, Please?" *The New York Times* (15 March 2001), online: The New York Times <http://www.nytimes.com/2001/03/15/technology/15BORD.html?pagewanted=all> (date accessed: 15 March 2001).

230 BBBOnLine, *General Privacy Seal Program Requirements*, *supra* note 198 at 1, clause 2 under Threshold Requirements, Eligible Organizations.

On the whole, the three seal providers examined would not be a precise fit if an on-line business wanted to have a third party declare its privacy *bona fides* by verifying that it meets the obligations set out under the *PIPA*. In some places, the three lag behind the *Act*; however, in other areas they exceed it. There seems to be an opening for a seal that uses the legislation as its bottom line and then builds upon it. Canadian web sites, or simply sites aimed at Canadians, could then trumpet their compliance with the *Act*. More importantly, because compliance should be automatic for sites under Canadian jurisdiction, they could signal a willingness to observe even stricter standards. This would acknowledge the existence of on-line privacy perils not contemplated by the law that are still worth addressing.

V. DEVELOPING A CANADIAN SEAL

Since the *PIPA* does not hold a monopoly on useful ideas in the area of data protection, the creators of a Canadian on-line privacy seal should take into account the progressive ideas advanced both by the trustmarks considered here and by their competitors. In addition, they would be compelled to examine the differences between federal private sector privacy legislation and similar provincial laws.[231] Where higher standards exist, the seal would be of no value unless it attained that level. Quebec is now the only province with its own legislation in place, but both Ontario[232] and British Columbia[233] intend to follow suit. These three provinces make up almost 75 percent of the population,[234] and thus a privacy seal that did not meet their standards would be without nationwide legitimacy.

Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*, for instance, has a stringent requirement for consent that requires it to be "manifest, free and enlightened" and given for specific purposes.[235] Once those purposes are achieved, the consent is no longer valid. Contrasting this standard with the rules set out in Schedule 1 of Bill C-54, as the *PIPA* was known when it was first introduced in Parliament,[236] Quebec's Access to Information Commission declared the latter "would constitute a step

---

231 On January 21, 2004, the *PIPA* will apply to all commercial information within a province, whether or not it is federally regulated, unless the province has adopted "substantially similar" legislation to the *Act*.

232 For preliminary information on Ontario's position, see Ontario, Ministry of Consumer and Commercial Relations, *supra* note 187.

233 British Columbia, Information, Science, and Technology Agency, *A Discussion Paper: Protecting Personal Information in the Private Sector* (British Columbia: October 1999), online: Information, Science, and Technology Agency <http://www.ista.gov.bc.ca/FOI_POP/PSP_100799.htm> (date accessed: 26 September 2000).

234 Based on 1996 census figures from Statistics Canada. Canada, "1996 Census of Canada - Population and Dwelling Counts" in *The Daily* (15 April 1997), online: Statistics Canada <http://www.statcan.ca/Daily/English/970415/d970415.htm> (date accessed: 29 December 2000).

235 S.Q. 1993, c. 17, P-39.1, *supra* note 117 at Division III, 1. 14.

236 *The Personal Information Protection and Electronic Documents Act* was introduced in the House of Commons in October 1998 as Bill C-54. However, it died on the order paper when Parliament adjourned. It was reintroduced as Bill C-6 when the next session of Parliament opened in October 1999.

backwards for the protection of the personal information of Quebeckers."[237] In total, the commission listed eight areas where, at that time, the proposed federal legislation differed from the provincial legislation. Some of these areas are explored below.[238]

Under the heading "Rules Respecting the Collection of Personal Information," the commission raised the issue of instances where policy that is mandated in Quebec is merely recommended at the federal level. Among other things, s. 8 of the provincial statute obligates the individual establishing a file containing personal information to explain the object or purpose of the file to the person concerned. In contrast, Principle 4.2.5 of Schedule 1 in the *Act* states: "Persons collecting personal information *should* be able to explain to individuals the purposes for which the information is being collected."[239] Some sites now offer contact with a customer service representative through typed "chats"[240] or through voice communications over Internet protocol ("IP").[241] Under the Quebec law, those people would be responsible for explaining the purposes of data collection. A second instance that demonstrates different data collection rules involves a business obtaining information about an individual from another business. Section 7 of the Quebec statute requires the source to be noted in the file, which is available to the data subject.[242] Principle 4.9.1 of the *Act* only encourages organizations to record the source of the information.[243]

When considering "Rules Respecting the Disclosure of Personal Information to Third Parties," the commission noted that s. 18(10) of the Quebec statute requires that subjects of a file be permitted access to an entry detailing the specifics of any information transfer that occurred without their consent.[244] Meanwhile, the *PIPA* Principle 4.9.3 of Schedule 1 assumes that a business may not be able to provide a precise list of organizations that have received information. The *Act* requires the business to supply a list of organizations "to which it may have disclosed information about the individual."[245]

---

237 Quebec, Access to Information Commission, *Opinion of the Commission d'Accès à L'information du Québec (Quebec Access to Information Commission) on Bill C-54 Personal Information Protection and Electronic Documents Act*, (Quebec: November 1998) at 15. Available directly from the commission office in English or on the Web in French only, online: Commission d'Accès à L'Information <http://www.cai.gouv.qc.ca/a981514.htm> (date accessed: 16 January 2001).

238 Although the commission was contrasting Quebec law with Bill C-54 as it was then proposed, the comments in the following section still apply. That is, amendments to Bill C-54 and later Bill C-6 did not invalidate any of the comparisons discussed.

239 *Supra* note 8 [emphasis added].

240 One such company is LivePerson online: Liveperson Homepage <www.liveperson.com>. Its list of 800 clients includes Cornell University, Timex, and Intuit. LivePerson also provides a service where customers enter a phone number and receive a traditional phone call.

241 Commonly known as Voice over IP or VoIP. Lipstream online: Lipstream Homepage <www.lipstream.com> is an example of this type of company. Customers include Excite@Home, Compaq, and American Express.

242 *Supra* note 117.

243 *Supra* note 8.

244 *Supra* note 117. Although both the Quebec statute and the *PIPA* generally do not permit disclosure of information to third parties without consent, there are occasions when it is allowed. In Quebec for instance, disclosures to the individual's attorney are permitted or to a person requiring the information in a situation where the data subject's life, health, or safety is threatened.

245 *Supra* note 8.

While discussing "Rules Respecting the Exercise of the Access Right," the commission criticized s. 8(4) of the bill because, in certain circumstances, the obligation to respond to a person's request to look at their file within thirty days may be extended by thirty days. Under s. 32 of the Quebec statute, "[f]ailure to respond within 30 days of the receipt of a request is deemed to be a refusal to grant the request."[246]

The commission also had concerns under the heading of "Citizens' Remedies." One concern was that the federal legislation shifts the burden of proof to citizens when there are disagreements about amending information in an individual's file. Section 53 of the Quebec statute requires that the entity holding the file prove it does not need amendment.[247] Conversely, the *PIPA's* Principle 4.9.5 of Schedule 1 states that an organization does not have to amend information until "an individual successfully demonstrates the inaccuracy or incompleteness of personal information."[248] This is a clear case in which identifying the higher standard is dependent on whether you approach the issue from a consumer or a business perspective. Clearly, a Canadian seal has to make a stand on the issue. It will be argued later in the article that identifying with the consumer point of view is the correct method. In the meantime, it is apparent that the seal project would have to carefully consider the implications of Quebec's legislation. In addition, it should not be long before Ontario has entered the private sector privacy arena.

Ontario is considering privacy protection that is broader than the *PIPA* because it would apply to non-profit organizations using information for purposes that would not be considered "commercial" under the *Act*.[249] Further measures that may be considered in Ontario can be found in an extensive list of Best Practices for Online Privacy Protection prepared by the province's Office of the Information and Privacy Commissioner.[250] Certainly, the commissioner could be expected to be an advocate on behalf of these principles. What follows is a selection of some of the most notable and novel of more than 100 suggestions made when compared with the *PIPA* and privacy seal programs:

- Recognize individuals as the owners of their own personal information.

...

- Assess the impact on privacy of any proposed new practice, service, product, or technology, prior to implementation. If the activity potentially will adversely impact privacy, do not do it, or find a less privacy-invasive way. Alternatively, fully advise individuals of the impact on privacy and obtain their explicit consent prior to proceeding.

...

246 *Supra* note 117.

247 *Ibid.*

248 *Supra* note 8.

249 Ontario Ministry of Consumer and Commercial Relations, *supra* note 187 at 3.

250 Exhibit B in A. Cavoukian, "Should the OECD Guidelines Apply to Personal Data Online?" (22nd International Conference on Privacy and Personal Data Protection, Venice, September 2000) online: Information and Privacy Commissioner/ONTARIO <http://www.ipc.on.ca/english/pubpres/sum%5Fpap/papers/oecd.htm> (date accessed: 3 December 2000).

- Prepare and post a privacy policy on your Web site.[251] That policy should clearly explain all your responsibilities and practices as outlined in these best practices. Specifically, it should be designed so it is:
  - o easy to find, easy to read, and easy to understand (e.g., use illustrative examples to explain and demonstrate your policy and practices);
  - o written in the same language as the Web site to which it is attached;
  - o accessible from every Web page, not just the homepage;
  - o easy to print; and
  - o necessary for the individual to click through and acknowledge it prior to commencing a transaction or the collection of any personal information.

...

- Collect no personal information, whenever possible (e.g., permit the individual to visit your Web site without capturing clickstream data, or let the individual deal with you anonymously or pseudonymously).

...

- Explain if individuals' personal information will be de-identified and used for data mining or other modelling processes prior to collection.

...

- Avoid collecting unique identifiers (e.g., SIN or driver's licence numbers) unless their use is required by law, or explicit consent is obtained from the individual. If required to collect unique identifiers (e.g., for tax requirements), explain reasons to the data subject prior to collection.

...

- Do not use clickstream data or any type of tracking technology or software without the explicit consent of the individual.[252]

The best practices listed above tend towards being limiting measures as opposed to efficiency measures. The first item is a cornerstone of this view. If consumers are the owners of their personal information, it follows that organizations should ask permission before doing anything with that property. The principle of collecting no information at all if possible is closely related to, and is certainly the antithesis of, an efficiency measure.

Consumers themselves, or the organizations that represent them, are yet another source of ideas whose merits should be considered for a trustmark. For example, among the thirty recommendations in a recent Consumers International[253] report was the following: "Information must be obtained directly from the consumer unless the consumer gives his or her prior consent allowing the information to be collected from another source."[254] The burden here is on the organization seeking additional information to secure consent from the consumer. This may be contrasted with TRUSTe's supplementation of

---

251 The final three subclauses are novel in this item.

252 *Supra* note 250. This listing of best practices is considered a draft version and is being revised for publication as a stand-alone paper according to e-mail correspondence from B. Spence, "Re: relevant vs. necessary." E-mail to J. MacDonnell (4 December 2000). Later published as Information and Privacy Commissioner/Ontario, "Best Practices for Online Privacy Protection" June 2001, online: <http://www.ipc.on.ca/english/pubpres/papers/bpon-e.htm> (date accessed: 15 August 2001).

253 Consumers International is a non-profit federation of 263 consumer organizations, online: Consumers International Homepage <http://www.consumersinternational.org/>.

254 Scribbins, *supra* note 129 at 8.

information policy, which places the responsibility on the consumer to act if they object to the collection of information about themselves from third parties.[255] Some, but not the majority, of the other policies suggested by Consumers International are also more stringent than those previously discussed from the trustmark programs and other sources. However, Consumers International is also the only one that specifies a few policies aimed at motivating consumer action and awareness. For example, "Consumers should consider the existence and content of a privacy policy before submitting personal data to a site."[256]

The emphasis on putting consumers first, found in the suggestions from the Ontario privacy commissioner and Consumers International, should be at the core of a privacy trustmark. At least it should be if the overriding purpose is to protect privacy rather than promote business. Otherwise, why should consumers take a trustmark provider at its word? In practice, the two objectives have always been intertwined, but this may not be the best way to allay consumer concerns. An Australian senate committee[257] has recommended the development of a privacy web seal by the federal privacy commissioner to certify that a site offers "the highest level of privacy protection from *the consumers' point of view.*"[258] It would use Australia's National Privacy Principles[259] as a minimum, but would be more stringent in some respects. That model makes sense in Canada as well. Legislation need not be the last word since a seal is voluntary, while meeting the legal standard is not. Therefore, a web site displaying a trustmark that allows consumers to easily determine that it exceeds the legislated minimum may have a marketing advantage.

As in Australia, Canada's federal privacy commissioner is uniquely positioned to develop and promote a privacy seal written primarily with consumers in mind. It could be a standard that concentrates on limiting collection measures before efficiency measures because it is the product of an organization with a mandate to protect citizens, not one seeking to increase sales by calming privacy concerns.

Admittedly, this notion diverges from what the Canadian E-Business Opportunities Roundtable envisions in its initial report.[260] First, the Roundtable aims to establish a set of "consumer protection guidelines" that not only encompasses privacy, but also include

---

255 *Supra* note 203 at 5, s. 3.1.5.

256 *Supra* note 253 at 10.

257 Australia, Senate, Select Committee on Information Technologies, "Cookie Monsters? Privacy in the information society" (November 2000), online: Parliament of Australia <http://www.aph.gov.au/senate/committee/it_ctte/e_privacy/> (date accessed: 6 November 2000).

258 *Ibid.* at 123 [emphasis added].

259 The privacy principles are available online: Australian Law Online <http://www.law.gov.au/privacy/NPP.html> and are part of Privacy Amendment (Private Sector) Bill 2000, which comes into effect 22 December 2001. The bill amends Australia's *Commonwealth Privacy Act* (1988) to bring private sector privacy under the umbrella of federal legislation.

260 In its second report, issued 13 months after the first, the Roundtable moves away from direct participation in the trustmark initiative after determining "that there may be better ways or other organizations capable of achieving the same objectives." Boston Consulting Group (Canada), "Fast Forward 2.0: Taking Canada to the Next Level" February 2001 at 10, online: Industry Canada <http://e-com.ic.gc.ca/english/documents/ff2.pdf> (date accessed: 16 March 2001).

broader concerns such as the merchantability of goods and the reliability of delivery.[261] Also, the development of this trustmark "should be led by the private sector" and be "managed by a neutral third party."[262] The office of the privacy commissioner should qualify as a neutral third party, but this is probably not what the business members of the Roundtable had intended. Business interests do not often see government as a neutral party. However, data protection authorities are usually at an arm's length from government and can be considered independent. Having the commissioner spearhead the initiative is definitely not in line with the proposal for the private sector to lead the seal project. However, there does not seem to be an urgent need for yet another seal-granting body that both polices industry and depends on it for financial support. According to one research firm's report, groups like TRUSTe and BBBOnLine are more privacy advocates for industry than for consumers because they earn their money from e-commerce organizations. What is needed in the United States, the report says, is a call from the FTC for a consumer-based organization to provide principles and redress.[263]

One appeal of a seal emanating from the office of the privacy commissioner is that it need not compete with the seals of TRUSTe, WebTrust, BBBOnLine, and their kind. Instead, it could be a "seal of seals" that verifies whether one of them, or an industry's code of practice, meets Canadian standards. This alternative could be a hybrid of a policy idea lifted from TrustUK,[264] a seal program endorsed by the British government, and a display idea taken from TRUSTe's EU Safe Harbor Privacy Program. TrustUK is a non-profit body that approves on-line codes of practice, but it does not directly endorse individual web sites. Instead, it certifies that the code of practice followed by whatever industry association or "subscriber body" to which the site belongs is compliant with its own standards. In the event of a conflict between a consumer and a site the complaint is lodged first with the site and then with the "code owner"[265] if a satisfactory resolution is not found. Lastly, TrustUK acts as an arbitrator if issues remain unresolved.

This British program was launched as a self-regulatory instrument by the Alliance for Electronic Business and the Consumers Association after a request from government in 1999. It was a response to fears that the proliferation of trustmarks, or *hallmarks* as the British prefer, would lead to confusion in the marketplace.[266] The TrustUK solution is to allow qualifying sites to display its mark, solely or in tandem, with the established mark of the association whose code it honours. Consumers who know what TrustUK

---

261 Boston Consulting Group (Canada), *supra* note 2 at 42.

262 *Ibid.* In this way, it would be closer to the WebTrust model than to TRUSTe or BBBOnLine.

263 Forrester Research report covered in article by C. Dembeck, "Report Labels Internet Privacy Policies a Joke" *E-Commerce Times* (16 September 1999), online: E-Commerce Times <http://www.ecommercetimes.com/news/articles/990916-3.shtml> (date accessed: 12 January, 2001).

264 As well as privacy, it also considers order fulfillment, payment security, and dispute arbitration. See the TrustUK web site, online: TrustUK Homepage <http://www.trustuk.org.uk/> (date accessed: 11 January 2001).

265 This is how TrustUK refers to the industry association or subscriber body that maintains the code of practice applicable to the web site.

266 From the section *Information on TrustUK* on the organization's web site, online: TrustUK <http://www.trustuk.org.uk/default.asp?option=1> (date accessed: 11 January 2001).

represents can then be confident that the code of practice for that site and, logically, the site itself meets their expectations.

For ease and clarity, it might serve the purposes of TrustUK, and any other seal overseer adopting its methods, to make the program's symbol an add-on to the trustmark of the approved code owner. Rather than displaying the TrustUK symbol in isolation or together with the symbol of the code owner, the two could be merged so that the former appears as a small tag appended to the top edge of the latter. This is how TRUSTe distinguishes its original trustmark from its newer Safe Harbor Privacy Program mark.[267] The top edge of the trustmark has an added tab which is about a sixth of its size. In this area is a small "plus" symbol, a simple logo depicting part of the northern hemisphere and the letters *E* and *U*. The obvious difficulty with this format is that while TRUSTe is a single organization operating two programs, this new hybrid logo would represent two organizations. Since clicking on a trustmark usually takes you to a site verifying the veracity of the mark,[268] it would have to be a two-step process in this case. It would make sense to be taken first to the verification site of the code owner. There, one would find an explanation of the code owner's program and information verifying that the originating site is a valid member of the program. This site would also display the mark of the seal overseer, which could be clicked in order to receive information authenticating that the code owner's program has been approved.

For the purposes of a Canadian seal, a code owner could be an industry association or it could be an entity such as TRUSTe, BBBOnLine, or WebTrust. The Canadian seal would certify that the code meets its standards, and then a tab with its logo would be added to the mark used by the code owner. It would be a registered certification mark under s. 23.(1) of the *Trade-marks Act*.[269] Perhaps the logo would be a stylized maple leaf accompanied by ".ca". While it is not the most original name, this program will be referred to as *CanTrust* for discussion purposes.[270]

An on-line seal appears to be a natural extension of the privacy commission's newly expanded duties to promote awareness of privacy issues in Canada and to encourage organizations to develop and adopt privacy policies. Since the office would not rely on the organizations displaying its seal for its principal source of funding, it would not risk being seen as beholden to those same businesses. The CanTrust standard would use the *PIPA* as a base and build from there. A more thorough version of the examination done for this article of the best policies from other seal providers and jurisdictions would

---

267 The Safe Harbor Privacy mark can be viewed online: TRUSTe <http://www.truste.org/programs/pub_harbor.html> (date accessed: 6 January 2001).

268 Alternatively, clicking a trustmark takes the user to the privacy policy and an additional link on that page brings up a verification screen.

269 R.S.C. 1985, c. T-13, online: Department of Justice <http://laws.justice.gc.ca/en/T-13/index.html> (date accessed: 23 June 2001).

270 This is probably not the wisest choice because it could tread on the trademark rights of TD Canada Trust, a retail banking operation. The domain name cantrust.com is registered to Canada Trust according to a WHOIS search undertaken on January 7, 2001. Network Solutions online: <http://www.networksolutions.com/cgi-bin/whois/whois>. As well, cantrust.ca is registered to CanTrust Financial Services Inc. of Coquitlam, British Columbia.

provide further criteria to ensure a consumer-oriented set of guidelines. The CanTrust symbol could then be appended to the logo of any code owner whose own policies qualify and who demands compliance with those policies by subscribers.

This position as a seal overseer would demand that the office of the privacy commissioner approach its work from two perspectives. The first would be as an educator and enforcer of the *PIPA*, the minimum acceptable level of data protection in the nation. The law would be the "stick" available to penalize transgressors. Meanwhile, the CanTrust seal would be a "carrot" used to reward organizations prepared to embrace privacy policies that transcend the *Act*. The government would even be able to point to the seal as evidence that legislation and self-regulation can be compatible. Although the *PIPA* does not contemplate such a scenario, there is nothing inherent in the legislation that would necessarily rule it out. Section 24(d) of Part I says the commissioner shall "promote, by any means that the Commissioner considers appropriate, the purposes of this Part."[271] This mandate is broad and may include promoting a standard that goes beyond the actual law. As well, the joint development of a CanTrust seal could offer a forum through which the provincial privacy commissioners and the federal office work to resolve any differences in their legislation.

At this point, the question of verifying compliance arises. In the standardization community it is commonly held that there are three steps to be observed: Say what you do; do what you say; and be willing to have it verified. The discussion of a CanTrust seal has to this point only addressed the first step. The seal would only be awarded to code owners whose subscribers are prepared to say that they will honour their commitments to the code, which are in line with CanTrust policies. However, it would still be necessary to verify that the promise was not just words on paper or, in this case, words on the Web. Therefore, one condition of being awarded the seal could be that the code owner requires regular privacy audits by all of its subscribers. The CanTrust authorities would have to outline exactly what constitutes an acceptable audit process. For instance, TRUSTe may not qualify for the CanTrust seal because its seeding of client web sites with unique identifiers is not a sufficiently rigorous test.

The *PIPA* gives the privacy commissioner an audit power under ss. 18 and 19.[272] It is to be used when there are reasonable grounds to believe that an organization is contravening a provision of the *Act* or not following a recommendation under Schedule 1. Considering this, the commissioner would not be in a position to audit organizations for compliance with a CanTrust seal. After all, it would be possible to respect the law but not follow all of the seal guidelines, which would require that the audit function be handled by outside agencies. Perhaps, CanTrust would have to approve various auditors or audit methods. Depending on the type of organization covered by a code owner, auditing standards may vary. A privacy audit for an organization in the health care field may differ substantially from one covering a company specializing in financial services. Both of these examples may involve audits more exacting than one conducted for an on-line hardware retailer where, presumably, much less sensitive information would be

---

271 *Supra* note 8.

272 *Ibid.*

concerned. The separation of audit responsibilities is in line with the "carrot and stick" approach. An audit by the office of the commissioner would signify that the data protection practices of an organization are suspect. No one would willingly seek out such a distinction. On the other hand, an audit to check conformity with CanTrust guidelines would be a sign that an organization is interested in not only meeting its obligations under the law, but also exceeding them. Of course, an audit could result in the revocation of the trustmark. However, it is reasonable to believe that most subscribers serious enough to seek the distinction would make an effort to maintain it.

The subject of auditing privacy practices deserves a much fuller examination, one that is beyond the scope of the present article. The obstacles to overcome are substantial. One obstacle is that there will always be a tension between the costs of a rigorous audit and the mass acceptance of a privacy standard. While a large organization may be willing to undergo an audit at considerable expense to itself, chances are that reluctance will be more apparent as the size of the entity decreases. Even in an organization that does its best to address privacy concerns, having to pay to prove compliance may not be feasible.

One solution to this particular problem has been advanced by Colin Bennett in a different context, and it involves three tiers which he labels: "1) A Conformity of Policy; 2) A Conformity of Procedure; and 3) A Conformity of Practice."[273] Only an organization in the third tier would undergo a complete privacy audit. In the circumstances theorized for a CanTrust seal, the first level would signify the code subscriber's self-declaration that it has adopted the policies as established by the code owner;[274] or *say what you do*. Conformity of Procedure would require objective verification that the policies had not only been adopted, but also that the organization's internal operating guidelines were in line with those policies; or *do what you say*. Finally, Conformity of Practice would involve a third party audit to verify that policies and procedures had been carried out as stated; or *be willing to have it verified*. The important thing to remember for all three of the tiers is that the code owner would be responsible for each one. They would not necessarily be responsible for conducting an audit; rather they would be responsible for ensuring that one is carried out. In the first two tiers, the code owner would be a logical party to ensure policies and procedures conform to the code. Matters would only be elevated to the CanTrust level in cases where a dispute could not be resolved between a code subscriber and a code owner.[275]

Essentially, there is a greater burden as an organization rises to a higher tier. At the same time, a readiness to be audited should indicate an intent to take data protection seriously. This intent would not be lost on the consuming public. However, organizations

---

[273] Bennett was commenting on conformity assessment possibilities if the CSA Model Code were adopted as a standard. C. Bennett, "Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada" (August 1997), online: Industry Canada-Electronic Commerce in Canada <http://www.e-com.ic.gc.ca/english/privacy/632d29.html> (date accessed: 20 August 2001).

[274] Also, indirectly, the policies of the CanTrust oversight seal.

[275] At the Conformity of Practice stage, matters of liability need to be closely considered. If an auditor verifies that a site conforms to the designated privacy practices but this assessment is found to be incorrect, would the auditor be liable for damages incurred by a third party? Would CanTrust?

with fewer resources would still have options. Communicating all of this effectively in a trustmark becomes increasingly complicated as more options become available. Perhaps each code owner would have access to three different CanTrust tabs: CanTrust,[1] CanTrust,[2] and CanTrust.[3] For example, CanTrust[1] would indicate Conformity of Practice.

Acceptance of a CanTrust seal may be slow at first, but the office of the privacy commissioner could use its position to expound the worthiness of the initiative and to offer assistance to organizations attempting to conform. If the standard became sufficiently well known, the public may begin to ask why organizations with which they deal fail to meet it. Even if masses of organizations do not adopt the standard, the very absence of the mark could serve as a flag that indicates best practices are not being followed. Consumers may then exert pressure to conform by directly voicing their concerns to the entity involved or by bypassing it altogether and doing business elsewhere.

A. TAKING THE INTERNATIONAL STAGE

In line with the objectives of the Canadian E-Business Opportunities Roundtable, the next step to consider would be to move a privacy oversight seal into the international arena. However, this inspires a vision of trustmarks from Australia, Britain, Canada, and elsewhere littering the web site of an on-line retailer that aspires to do business in any of those nations. However, the intention is that seals be visible so that they act as a quick reminder of the privacy provisions of a particular site. A plethora of seals could run counter to this goal by either crowding the visual field on a consumer's screen or by dissuading organizations from using them in the first place. Having to meet the criteria of disparate seals from a number of nations would surely not be a priority. Of course, each nation may simply hope to have the seal adopted at home. However, this appears to be counterintuitive for use on a platform known as the World Wide Web. Also, it certainly conflicts with the the aspirations of the Canadian E-Business Opportunities Roundtable, which foresees "an internationally recognized trustmark."[276] TrustUK also has ambitions beyond the shores of Britain.[277]

The concept of adding a CanTrust tab to the logos of certified trustmarks, or marks associated with a particular industry code, may help alleviate the privacy seal clutter. But if other jurisdictions followed suit, each approved mark would suddenly be inundated with tabs. Still, this may be a better solution than various separate marks, and it would quickly establish the site's code owner and the identity of the overseer or overseers.

The ultimate solution could be for the countries that have established such a program, or that are contemplating one, to cooperate in the development of a single international standard. What better body of people to devise and administer such a standard than the group already tasked with protecting the personal information of citizens: privacy

---

[276] Boston Consulting Group (Canada), *supra* note 2 at 42.

[277] The government hopes to "market the e-commerce hallmark internationally." See UK Department of Trade and Industry, "Modern Markets: Confident Consumers" (1999), online: Department of Trade and Industry <http://www.dti.gov.uk/consumer/whitepaper/chap4.htm> (date accessed: 6 January 2001).

commissioners in jurisdictions around the world?[278] Some commissioners are already moving towards greater international cooperation. A prime example of this cooperation is the recently launched Virtual Privacy Office.[279] This office is an attempt to pool the resources of privacy protection officials, provide them with an on-line presence to educate the public, and allow them to gain greater experience with the Internet technologies that threaten privacy on a scale unimagined only a decade ago.[280] It is an initiative of the privacy commissioner of Schleswig-Holstein, Germany. As of January 2001, it also involves privacy commissioners from Zurich, Switzerland, Ontario, the Dutch Data Protection Authority, and all of Germany's state and federal governments.[281] Participation is open to all privacy protection authorities. Ontario's privacy commissioner, Ann Cavoukian, urged other commissioners to get involved in a fall 2000 report presented at their annual conference.[282]

An on-line privacy seal does not appear to be on the agenda of the Virtual Privacy Office, but it would be a logical project for the new organization to undertake. However, this is based on the assumption that the respective governments who finance the various privacy offices would support their participation in the scheme. This would allow the program to be run on a cost-recovery basis for the approval of an individual code. With a critical mass of privacy and data protection offices taking part, however, this one-for-all approach should not place an undue burden on the resources of any one office.

VI. CONCLUSION

Privacy is a slippery concept, both in terms of defining it and retaining it. The issue that has been explored here — information privacy or data protection — is perhaps the hardest to grasp. In simpler times, an invasion of privacy constituted someone physically knocking down your door and entering your home; not welcome, but obvious. Developing technology has consistently made it easier to distance the invader from the victim. With cameras, the target had to be in sight. The introduction of wiretaps meant you did not even have to be in earshot. At the present time, people routinely traverse digital domains and shed data along the way. Information, mostly anonymous, some not, and some that could be massaged into personal information, is effortlessly swallowed up in databases nearby and around the world. In an information economy, that data is the coin of the

---

278 January 2001 saw calls from two fronts for the creation of an international consumer protection body with jurisdiction over privacy. See Scribbins, *supra* note 129 at 15 and D. McGuire, "Nader Wants International Body to Protect Consumers Online" (9 January 2001), online: Newsbytes.com <http://www.newsbytes.com/news/01/160265.html> (date accessed: 10 January 2001).

279 The Virtual Privacy Office went online December 5, 2000. Privacy Service, online: Privacy Service Homepage <http://www.privacyservice.org/>. See also S. Kettman, "Do You Even Know Who's Watching?" *Wired News* (11 January 2001), online: Wired News <http://www.wired.com/news/print/0,1294,40935,00.html> (date accessed: 11 January 2001).

280 B. Baeriswyl *et al.*, "The Virtual Privacy Office — A New Approach To Privacy Protection" (Submission to Information Security Solutions Europe Conference, Barcelona, 27-29 September 2000), online: <http://www.datenschutz.parlanet.de/institutionen/virdsb/isse00tx.pdf> (date accessed: 6 October 2000).

281 Another participant is the privacy commissioner of the Roman Catholic dioceses in northern Germany.

282 Cavoukian, *supra* note 250 at 21.

realm. Business covets it, but wary privacy advocates caution that so much is flowing so freely that a disaster is waiting to happen — a privacy Chernobyl.

In Canada the federal government has added some friction to decrease that flow in the form of the *Personal Information Protection Act*. It is an awkward amalgam that uses the CSA Model Code as a platform on which to build private sector privacy legislation. In most respects, it comes out well when contrasted with three prominent trustmarks that are exemplars of the American self-regulatory approach. As law, its chief advantage is that it will apply across the board. No matter how impressive the policies of the trustmark programs are, their reach is far exceeded by the number of web sites that display no such seal. A disadvantage of the *Act* when applying it online is that it does not explicitly anticipate some of the issues that are unique to that environment. The requirement that any collection, use, or disclosure of information must be for purposes that a reasonable person would consider appropriate allows a broad scope to address that omission. Still, a trustmark provides a way to promote good data protection on the Web that may transcend Canadian borders in a way the law is unlikely to. As proposed, the CanTrust program could even encourage the adoption of privacy policies that transcend the law.

Does e-commerce need a Canadian privacy seal of approval? In the short term, the answer is yes. But the model proposed by the Canadian E-Business Opportunities Roundtable may not be the correct one. Rather than have the private sector in control, an organization with consumers' interests in mind should be at the forefront. Otherwise, the effort amounts to business deciding how far it should reluctantly go to placate privacy fears. The goal should be to strive for a standard under which consumers have nothing to fear. Coincidentally, as various studies point out, greater privacy protection should increase on-line business, which is a laudable goal. Greater economic opportunities are not undesirable. However, achieving a more privacy-friendly society is a matter of upholding what has been recognized as a basic human right.[283] Perhaps the order of priority should be data protection first — and *then* business. From the implementation of the OECD *Guidelines* onwards, business interests have been put on an equal footing with privacy concerns. The EU *Directive* was prompted by fears that trade barriers within Europe would be erected because of a patchwork of differing national privacy laws. In turn, the extraterritorial aspect of the *Directive's* demand for "adequate" protection for transborder data flows pushed non-European jurisdictions to take action. The *PIPA* in Canada and Safe Harbor in the United States are only two of the results. However, in all cases the issue turned more on protecting pocketbooks than privacy. It is as if, in 1928, Judge Louis Brandeis had proclaimed, "Capitalism is the most comprehensive of rights, and the right most valued by civilized men."

Of course, it would be naive to ignore business interests in the design of a privacy seal. A voluntary standard set at a level that no one is prepared to meet would become a superfluous theoretical exercise. The goal should be for a privacy mark that tips the scales

---

[283] See Article 12 of the United Nation's *Universal Declaration of Human Rights*, GA Res. 217 (III), UN GAOR, 3d Sess., Supp. No. 13, UN Doc. A/810 (1948) 71, online: United Nations <http://www.un.org/Overview/rights.html> (date accessed: 15 March 2001).

on the side of consumers, while ensuring that business or other organizations with an appetite for data are still willing to cooperate. The office of the federal privacy commissioner could be the organization to achieve that delicate balance. Its provincial counterparts would also be logical participants. Perhaps the same type of broad coalition of government, industry, and consumer groups that devised the CSA Model Code in the early 1990s could be fashioned. However, this time participants would be able to take into account the changes wrought by the Internet.

In the long term, a Canadian privacy seal would have to be supplanted by a mark signifying the co-operative efforts of an international group of data protection commissioners, aided by similar input from governments, industry, and consumers. There is no sense in being parochial when the citizens of any country can virtually travel to any other nation and carry out transactions at the click of a mouse. In the end, the standard that emerged would be similar to the OECD *Guidelines* or the *PIPA*, with the addition of criteria acknowledging the ability of the Internet to intensify potential privacy problems. Where private sector laws existed, legislators and the courts would be responsible for maintaining a privacy floor — a level that organizations must respect. Meanwhile, the seal would represent a higher level that organizations would be encouraged, but not obligated, to shoot for. At the same time, consumers would be further educated on privacy issues so that they could make informed choices.

In an increasingly networked world, such a trustmark would help alleviate the trade of personal information that threatens to wash away the very notion of privacy. It would not be a substitute for legislative or technological tools in aid of the same goal. Rather, it will take a concerted effort on all of those fronts to ensure that individuals really can claim "to determine for themselves when, how, and to what extent information about them is communicated to others."

APPENDIX 1: THE OECD GUIDELINES*

*Taken from *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), online: OECD <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>

Basic Principles of National Application

(1) Collection Limitation Principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(2) Data Quality Principle - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(3) Purpose Specification Principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(4) Use Limitation Principle - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 3 except:

a) with the consent of the data subject; or
b) by the authority of law.

(5) Security Safeguards Principle - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

(6) Openness Principle - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

(7) Individual Participation Principle - An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
   - o within a reasonable time;
   - o at a charge, if any, that is not excessive;
   - o in a reasonable manner; and
   - o in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs *(a)* and *(b)* is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

(8) Accountability Principle - A data controller should be accountable for complying with measures which give effect to the principles stated above.

APPENDIX 2: THE FTC'S FIPS FOR THE WEB*

*Taken from United States, Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) at 36-37, online: Federal Trade Commission <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>

All consumer-oriented commercial Web sites that collect personally identifying information from or about consumers online would be required to comply with the four widely accepted fair information practices:

(1) Notice - Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (*e.g.*, directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.

(2) Choice - Web sites would be required to offer consumers choices as to how their personally identifying information is used beyond the use for which the information was provided (*e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

(3) Access - Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.

(4) Security - Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.

The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations.

APPENDIX 3: SCHEDULE 1 OF THE *PIPA**

*Taken from the *Personal Information and Protection of Electronic Documents Act* — Schedule 1, S.C. 2000, c. 5, online: <http://laws.justice.gc.ca/en/P-8.6/79968.html>

4.1 Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1 Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4 Organizations shall implement policies and practices to give effect to the principles, including

(a) implementing procedures to protect personal information;
(b) establishing procedures to receive and respond to complaints and inquiries;
(c) training staff and communicating to staff information about the organization's policies and practices; and
(d) developing information to explain the organization's policies and procedures.

4.2 Principle 2 - Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6 This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 **Principle 3 — Consent**

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note:* In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

---

* Section 2(2) of Part 1 of the *PIPA* excludes the note under clause 4.3 from the law. Instead, s. 7 of Part 1 details the circumstances in which personal information may be collected, used or disclosed without the knowledge or consent of the data subject.

4.3.2 The principle requires "knowledge and consent." Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7 Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 **Principle 4 - Limiting Collection**

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3 This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 **Principle 5 - Limiting Use, Disclosure, and Retention**

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

4.5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4 This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 **Principle 6 — Accuracy**

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 **Principle 7 — Safeguards**

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3 The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;
(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
(c) technological measures, for example, the use of passwords and encryption.

4.7.4 Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1 Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2 The information made available shall include

(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
(b) the means of gaining access to personal information held by the organization;
(c) a description of the type of personal information held by the organization, including a general account of its use;
(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
(e) what personal information is made available to related organizations (*e.g.*, subsidiaries).

4.8.3 An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 - Individual Access**

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note:*** In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that

---

** This is affected by s. 8 of the Act: (3) An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request. (4) An organization may extend the time limit.

*** Section 2(2) of Part 1 of the *PIPA* excludes the note under clause 4.9 from the law. Instead, s. 9 of Part 1 details the circumstances in which access may be denied.

cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2 An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4 An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 **Principle 10 - Challenging Compliance**

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1 The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2 Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3 Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4 An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

APPENDIX 4: BBBONLINE

*Principles from Schedule 1 of the *PIPA*; Criteria 1-31 are authors own analysis of the principles; BBBOnLine listing, see *supra* notes 196, 198 of this article.

PIPA	BBB*OnLine*	Pts
Accountability Principle: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.		
1. Data controller(s) accountable for compliance with principles	**General Privacy Seal Program Requirements** **Threshold Requirements** **General Conditions** 5. A specific individual has been charged with the responsibility for implementing and overseeing the *privacy notice* for the website or online service. **Contract Conditions** 2. The organization agrees to participate in BBB*OnLine*'s Privacy Program Dispute Resolution Process, and to abide by decisions entered in that program. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 24. Individual Responsibility Since a privacy notice is not self-implementing, an individual within your organization's structure must also be assigned for enacting and implementing the notice.	1
2. Data controller(s) identity available on request	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 12. The *privacy notice* provides *contact* information for the organization in the instance there are questions or concerns about the organization's privacy and security policies. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 12. Contact Your Organization The explanation should include contact information, e.g., a phone number or email address, that will lead a person with a complaint about the treatment of his/her information to a person responsible for the receipt of such complaints without undue delay. In most cases, this means that a person calling during normal business hours should be able to speak to such a person during that first call or by the end of the next business day. This does not require that the issue be resolved in that time frame but simply that the individual has the opportunity to make an initial contact with a person authorized to take information regarding the privacy notice and begin the process of resolving it.	1

PIPA	BBB*OnLine*	Pts
3. Contractual or other means used to assure comparable protection of information transferred to third parties for processing	**General Privacy Seal Program Requirements** **Sharing of Information** 1. The organization requires *agents or contractors* who have access to *personally identifiable information or prospect information* to honor the organization's privacy and security policies, hold such information in confidence, and not use such information for any purpose other than to carry out the services they are performing for the organization. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 4. Agreements with Agents and Contractors The agreement you make with agents and contractors can be in whatever form will serve the purpose of requiring the agent or contractor to hold the information in confidence, not use it for any purpose except to carry out the service they are providing your organization, and to honor your organization's privacy and security policies in the way that information is handled. For example, it may be a specific commitment to follow your privacy and security policies or a commitment to treat the information as proprietary information of your organization.	1
Identifying Purposes Principle: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.		
4. Specify purposes to data subject at or before time of collection	**BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 26. Link to Your Privacy Notice Your privacy notice must be easy to find. At the very least, the privacy notice must be accessible by a clearly labeled link from your homepage(s) and every subsequent point where you elicit *personally identifiable information* and *prospect information* online through means other than passive data collection. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 65. Uses A website or online service must disclose in its privacy notice all of the types of uses and transfers of *personally identifiable information* then applicable to the personally identifiable information being collected (actively or passively) at the site or service. There must be sufficient information for the individual to be reasonably informed as to what uses will be made of the information...	1
Consent Principle: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.		
5. Knowledge and consent of data subject	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **General** 1. The *privacy notice* is easy to read, easy to find and appears (at least) through a clearly labeled and direct ("one-click-away") link on all the	1

PIPA	BBB*OnLine*	Pts
	homepages of the site or service, all areas at which the organization collects *personally identifiable information*, and all areas on the *covered website or online service* where an email address is held out for the organization. 2. The *privacy notice* lists all required disclosures in a single document. **BBB*OnLine* Privacy Program Assessment Questionnaire Help Document** 45. Privacy Notice A privacy notice is a written statement advising the public of the collection and use of *personally identifiable information* and security practices of your organization. A good privacy notice is easy to find, easy to read, and comprehensively explains all of your organization's online information practices. This notice provides online visitors an opportunity to make informed decisions about the collection and use of their information. The terms of the privacy notice are very important because they substantially determine an individual's understanding of how information will be used and what steps the individual may take to protect his or her privacy. A good privacy notice is tailored to the specific information practices of your organization and should not be merely copied from another source. 46. Prominent In addition to the general requirement for your privacy notice to be easy to read and easy to find, you must also make your privacy notice, or the links leading to your privacy notice "prominent." This means that the link or notice visually stands out from the rest of your website or online service and is readily noticeable. For example, a link appearing in a larger font size in a different color on a contrasting background would be considered prominent. "Prominent" would not be a link in small print at the bottom of a page, or a link that is indistinguishablefrom a number of adjacent links. 63. Types An important function of a privacy notice is to inform individuals what information is being collected about them with sufficient specificity for them to understand and make informed choices about the use of the website(s) or online service(s). The level of specificity in the language should prevent the average user that reads your notice from being surprised by what may be collected. It need not spell out every specific piece of information collected, but it must be enough to allow individuals to make an informed choice about the use of your website. We ask that your privacy notice include a comprehensive list of types of *personally identifiable information* or *prospect information* that your website collects online. This may include personal identifiers like names and email addresses, information about websites that have been visited where linked to email addresses or other specific identifiers, information about purchases, information about preferences.	

PIPA	BBB*OnLine*	Pts
	65. Uses A website or online service must disclose in its privacy notice all of the types of uses and transfers of *personally identifiable information* then applicable to the personally identifiable information being collected (actively or passively) at the site or service. There must be sufficient information for the individual to be reasonably informed as to what uses will be made of the information. For example, "We use this information to better understand your needs and provide you better service" is not sufficient disclosure of an intent to use the information to market to the individual. In addition, if the site(s) or service(s) transfers any of this information to unaffiliated third parties or corporate affiliates not governed by a common privacy notice for the marketing purposes of those parties, that fact must be specifically stated in its privacy notice. Examples of uses include order fulfillment, record keeping, direct marketing, or making information publicly available through a chat room or bulletin board.	
6. Product or service cannot be denied if data subject refuses to divulge information beyond that required for specified, legitimate purpose	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 15. If access to any part of the site or service is conditioned on the disclosure of *personally identifiable information*, and this is not also explained at the initial point of collection, the *privacy notice* discloses this fact. **General Privacy Seal Program Requirements** **Choice & Consent** 5. Where the website conditions the granting of access to some or all of its website(s) or online service(s) based on the disclosure of *personally identifiable information*, the organization must inform individuals, in its *privacy notice* or at the point of collection, of the consequences of refusing to provide such information.	1
7. Data subject may withdraw consent	**General Privacy Seal Program Requirements** **Choice & Consent** 1. Where an organization uses *personally identifiable information* for its own direct marketing, it provides individuals with the opportunity to *opt-in or opt-out* of this direct marketing at any time. **General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 9. When *personally identifiable information* or *prospect information* is shared with *outside parties or corporate affiliates* with different privacy notices, an organization's *privacy notice* discloses this sharing, the types of outside parties or corporate affiliates, and how individuals may prevent this transfer by opting-in or opting-out.	1

PIPA	BBB*OnLine*	Pts
	BBB*OnLine* Privacy Program Assessment Questionnaire **Help Document** 33. Opt-in or Opt-out Regardless of the disclosure an organization makes in the privacy notice about its practice of renting, selling, exchanging or in any way providing personally identifiable information for marketing purposes, an organization that makes such transfers to outside parties must provide individuals with the ability to prevent these transfers in connection with personally identifiable information about them. Providing individuals with an opt out will satisfy this requirement. It can also be satisfied by an opt in or, when technological tools that enable individuals to make choices about transfers become available, by the use of such tools as are determined by BBB*OnLine* to satisfy its requirements.	1
Limiting Collection Principle: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.		
8. Data collection limited to that necessary for identified purposes	**General Privacy Seal Program Requirements** **Threshold Requirements** **Contract Conditions** 1. An organization must take appropriate steps to assure that its information management practices comply with its privacy policies and any applicable BBB*OnLine* Privacy Program requirements ...	1
9. Data collection only by lawful and fair means	**General Privacy Seal Program Requirements** **Threshold Requirements** **Eligible Organizations** 4. Organizations must be engaged in activity that is legal, ...	0.5
Limiting Use, Disclosure, and Retention Principle: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.		
10. Use and disclose in accordance with specified purposes	**BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 65. Uses A website or online service must disclose in its privacy notice all of the types of uses and transfers of *personally identifiable information* then applicable to the personally identifiable information being collected (actively or passively) at the site or service. There must be sufficient information for the individual to be reasonably informed as to what uses will be made of the information. For example, "We use this information to better understand your needs and provide you better service" is not sufficient disclosure of an intent to use the information to market to the individual. In addition, if the site(s) or service(s) transfers any of this information to unaffiliated third parties or corporate affiliates not governed by a common privacy notice for the marketing purposes of those parties, that fact must be specifically stated in its privacy notice. Examples of uses include order fulfillment, record keeping, direct marketing, or making information publicly available through a chat room or bulletin board.	1

PIPA	BBB*OnLine*	Pts
11. Except with data subject consent or by authority of law	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 9. When *personally identifiable information* or *prospect information* is shared with *outside parties or corporate affiliates* with different privacy notices, an organization's *privacy notice* discloses this sharing, the types of outside parties or corporate affiliates, and how individuals may prevent this transfer by opting-in or opting-out. **General Privacy Seal Program Requirements** **Choice & Consent** 3. An organization provides individuals the opportunity to opt-out or otherwise prohibit any use of information about them that was not permitted in the privacy notice in effect at the time the information was collected or that is unrelated to the purpose for which the information was collected (see list of four exceptions). 4. The organization provides individuals with a choice regarding the transfer of information to *outside parties or corporate affiliates* operating under a different *privacy notice*. This may be accomplished through one or more of the following: i. an opt-out opportunity ii. an opt-in opportunity iii. through a technological tool for individuals to make choices about such transfers. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 20. Four Excepted Uses There are four uses of information that BBB*OnLine* does not require to be disclosed in the privacy notice. An applicant can include these uses in the privacy notice if he/she wishes, but they are not strictly required by the program standards. These four excepted uses are: a) Uses which are necessarily incident to one already described in the privacy notice (such as giving shipping information to the postal carrier in order to fulfill an order, when the privacy notice has already disclosed that shipping information will be used to fulfill the order). b) Uses which are required of the applicant by law (such as responding to a valid subpoena, warrant, audit, or agency action). c) Uses of information for research activities, including the production of statistical reports — as long as such information is not published, divulged, or used to contact the subjects of the report.	1

PIPA	BBB*OnLine*	Pts
	d) Uses of information in the context of a business transaction such as a merger, acquisition, consolidation, or divestiture — pursuant to a pledge of confidentiality under which the recipient agrees to use the information for no purpose other than carrying out the transaction.	
12. Data retained only as long as necessary for specified purposes		0
13. New uses of personal information shall be documented		0
Accuracy Principle: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.		
14. Accurate, complete and up-to-date as necessary for specified purposes	**General Privacy Seal Program Requirements** **Security** 3. The organization takes reasonable steps to assure that *personally identifiable information* and *prospect information* is accurate, complete, and timely for the purposes for which it is used. **BBBOnLine Privacy Program Assessment Questionnaire** **Help Document** 6. Assuring the Accuracy of Information In addition to providing individuals with the ability to correct factual inaccuracies in their personally identifiable information or prospect information, your organization must also take reasonable steps to assure that the individually identifiable information and prospect information that it collects is accurate, complete, and timely for the purposes for which it is used.	1
Safeguards Principle: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.		
15. Appropriate security safeguards	**General Privacy Seal Program Requirements** **Security** 1. The organization takes reasonable steps to ensure that *personally identifiable information* or *prospect information* is safe from unauthorized access, either physical or electronic. These steps include at least the following: a) The organization maintains *logs* to properly track information and assure that data is only accessed by authorized individuals. b) The organization maintains a written data security policy. c) The organization performs at least an annual review of its written data security policy. d) The organization provides adequate training for employees, agents, and contractors. e) The organization stores information in a secure environment (using features such as doors, locks, and electronic security). 2. Encryption is used whenever Type I sensitive information (such as financial transaction information like credit card numbers, social security numbers, or health-care information) is transmitted or received online.	1

PIPA	BBB*OnLine*	Pts
	BBB*OnLine* Privacy Program Assessment Questionnaire **Help Document** 5. Appropriate Security Your organization is required to take appropriate data security measures to protect personally identifiable information and prospect information. These measures must include physical security measures such as doors, locks, etc., as well as electronic security and managerial controls that limit the potential for unauthorized access or misuse by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by your organization's collection and use of the data. 11. Commitment to Online Data Security Although an organization is not required to provide a description in its privacy notice(s) of the specific data security measures it undertakes to protect *personally identifiable information*, it is required to take appropriate data security measures and to inform the public that such measures are in place by a statement in its privacy notice. The security measures must include physical security measures such as locked doors and files, etc., electronic security and managerial controls that limit the potential for misuse of information by employees and contractors. The security measures necessary to protect information sufficiently will vary based on the risks presented to the individual by the organization's collection and use of the data.	
Openness Principle: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.		
16. Ready access for data subject to policies and practices	**General Privacy Seal Program Requirements** **Threshold Requirements** **General Conditions** 2. The organization has adopted and implemented an online *privacy notice* (including an effective date) and posted this notice on the website or online service. **General Privacy Seal Program Requirements** **Privacy Notice Requirements** **General** 1. The *privacy notice* is easy to read, easy to find and appears (at least) through a clearly labeled and direct (6one-click-away") link on all the *homepages* of the site or service, all areas at which the organization collects *personally identifiable information*, and all areas on the *covered website or online service* where an email address is held out for the organization. 2. The *privacy notice* lists all required disclosures in a single document.	1
17. Policies and practices available in generally understandable form	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **General** 1. The *privacy notice* is easy to read ...	1

PIPA	BBB*OnLine*	Pts
18. Ready access to description of type of personal information held, including general account of its use	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 2. The *privacy notice* describes all the *types* of *personally identifiable information* or *prospect information* that may be collected through the website or online service (including email correspondence). If no personally identifiable information or prospect information is collected then the privacy notice notes this fact. 3. For each type of *personally identifiable information* or *prospect information* collected, the *privacy notice* clearly discloses how that information will be subsequently *used* and shared. Such uses may include, but are not limited to, order fulfillment, record keeping, marketing, or making it publicly available through a chat room or by other means. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 65. Uses A website or online service must disclose in its privacy notice all of the types of uses and transfers of *personally identifiable information* then applicable to the personally identifiable information being collected (actively or passively) at the site or service. There must be sufficient information for the individual to be reasonably informed as to what uses will be made of the information...	1
19. Ready access to description of what personal information made available to related organizations	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 3. For each type of *personally identifiable information* or *prospect information* collected, the *privacy notice* clearly discloses how that information will be subsequently *used* and shared. Such uses may include, but are not limited to, order fulfillment, record keeping, marketing, or making it publicly available through a chat room or by other means. 17. If there are other organizations that reside on a seal applicant's website or online service and collect *personally identifiable information* or *prospect information* from individuals while they remain on the website or online service then the *privacy notice* discloses the fact that these other organization are collecting information. The privacy notice identifies these other organizations and provides a URL (or some other form of contact information) that would allow the individual the opportunity to evaluate the privacy and security policies of these other organizations. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 65. Uses In addition, if the site(s) or service(s) transfers any of this information to unaffiliated third parties or corporate affiliates not governed by a common	1

PIPA	BBB*OnLine*	Pts
	privacy notice for the marketing purposes of those parties, that fact must be specifically stated in its privacy notice. Examples of uses include order fulfillment, record keeping, direct marketing, or making information publicly available through a chat room or bulletin board.	
Individual Access Principle: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.		
20. Data subject informed of existence, use, and disclosure of personal information	**BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 1. Access If your organization collects and maintains *personally identifiable information* or *prospect information*, then it must make this information available to the subjects of the information upon reasonable request and proper verification. Your organization has substantial flexibility in deciding the best way to provide access. However, this process must allow the subjects of the information access to ALL the information about them that is 1) maintained, 2) retrievable in the ordinary course of business, and 3) meets the definition of personally identifiable or prospect information.	1
21. Data subject can access personal information	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 5. The privacy notice clearly explains "how" a data subject may *access* (review) all their *personally identifiable information* or *prospect information* that the organization maintains in *retrievable form*. 10. If *personally identifiable information* and *prospect information* are collected, and not maintained in *retrievable form*, the *privacy notice* discloses this fact. **General Privacy Seal Program Requirements** **Access and Correction** 2. The organization has in place a process for providing *access* by making all *personally identifiable information* and *prospect information*, maintained in *retrievable form*, available to the subject of that data upon request.	1
22. Personally identifying information disclosed to gain access to information shall be used for no other purpose		0
23. Data communicated within 30 days and at a minimal or no cost to the individual	**General Privacy Seal Program Requirements** **Access & Correction** 1. The organization has in place a process, unlimited by frequency or fee, by which factual inaccuracies in *personally identifiable information* and *prospect information* maintained in *retrievable form* may be corrected upon request.	0.5

PIPA	BBB*OnLine*	Pts
	BBB*OnLine* Privacy Program Assessment Questionnaire **Help Document** 21. Frequency or Fee Limits Your organization may set reasonable terms under which it will make information available for access — such as through limits on the frequency of requests or through the imposition of fees. However, frequency limits that require intervals of more than a year between requests and/or fees of more than $15 for a response to a request would not be considered reasonable except in extraordinary circumstances.	
24. Requested information must be in form that is generally understandable		0
25. Reasons for denying access set out along with any available recourse	**General Privacy Seal Program Requirements** **Access and Correction** 4. For all *personally identifiable information* or *prospect information* to which an organization cannot provide access, either because it is not maintained in *retrievable form*, or it cannot meet any reasonable *frequency or fee limits*, the organization provides: a) an explanation why access cannot be provided, b) a contact for further information, and c) reference to the provisions in your privacy notice that discuss the *type* of data collected and how it is *used*, or provide the individual with materials on these matters that are at least as complete as the information provided in the privacy notice. **BBB*OnLine* Privacy Program Assessment Questionnaire** **Help Document** 1. Access If an organization cannot make information that it maintains available because it can not retrieve the information in the ordinary course of business, it must provide that individual an explanation why access cannot be provided, a contact for further inquires [*sic*], and a reference to the provisions in its privacy notice that discuss the type of data collected, how it is used, and appropriate choices related to that data, or, provide the individual with materials on these matters that are at least as complete as the information provided in the privacy notice.	1
26. Ability to challenge and amend	**General Privacy Seal Program Requirements** **Privacy Notice Requirements** **Privacy Notice Content** 6. The privacy notice clearly explains "how" a data subject may make factual *corrections* (update) all their *personally identifiable information* or *prospect information* that the organization maintains in retrievable form.	1

PIPA	BBB*OnLine*	Pts
	BBBOnLine Privacy Program Assessment Questionnaire **Help Document** 15. Correction Upon the request of an affected individual, an organization must correct factual inaccuracies in the personally identifiable information or prospect information it maintains about him or her, if the information will be communicated to others or used for substantive decision-making. The organization may choose the form of the showing that an individual must make to suggest the likelihood of a factual inaccuracy in the personally identifiable information that it maintains.	
27. Where appropriate, amended information passed on to third parties with access		0
28. Substance of unresolved challenges to information shall be recorded		0
29. Where appropriate, existence of unresolved challenges transmitted to third parties with access		0
Challenging Compliance Principle: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.		
30. Data subject can challenge compliance with principles	**General Privacy Seal Program Requirements** **Threshold Requirements** **Contract Conditions** 2. The organization agrees to participate in BBB*OnLine*'s Privacy Program Dispute Resolution Process, and to abide by decisions entered in that program. 3. The organization agrees to cooperate with BBB*OnLine* Privacy program verification requirements. Verification requirements include, but are not limited to, information pertaining to: choice, individual access to data, transfer of information to third parties, data integrity, security, and parental notice and consent (if applicable). **BBB*OnLine* Privacy Program Participation Agreement** D. Verification Licensee agrees to cooperate with BBB*OnLine* in verification of Licensee's compliance with Eligibility Requirements and this Agreement. BBBOnLine	1

PIPA	BBB*OnLine*	Pts
	may itself, or through an independent third party designated by BBBOnLine, conduct random compliance reviews (online, on-site, or otherwise) of one or more Eligibility Requirements on BBBOnLine's own initiative or in response to complaints from individuals or third parties (Random Review).	
31. Justified complaints addressed by appropriate measures, including, if necessary, amending policies and practices		0
	TOTAL	22

APPENDIX 5: TRUSTE

*Principles from Schedule 1 of the *PIPA*; Criteria 1-31 are author's own analysis of the principles; TRUSTe listings, see *supra* notes 202-205 of article.

PIPA	TRUSTe	Pts
Accountability Principle: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.		
1. Data controller(s) accountable for compliance with principles	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 2. A. Site Coordinator. Licensee shall name a coordinator for the Site (the "Site Coordinator") on or by the Effective Date of the Agreement. The Site Coordinator shall be the person responsible for the accuracy of the Privacy Statement and Implementation of the TRUSTe Program. 4. Reviews. Licensee shall reasonably cooperate with TRUSTe to ensure compliance with the Program, Program Requirements and Privacy Statement(s). TRUSTe may, itself or through an independent, qualified, neutral third party designated by TRUSTe, review the Privacy Statement(s) and the Site periodically, to assess the level of consistency and quality of use of the TRUSTe Mark(s) on the Site and the consistency and quality of Licensee's Privacy Statement(s) and related privacy practices, and Licensee's conformance with the Program Requirements throughout the term of the Agreement.	1
2. Data controller(s) identity available on request	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 2.F.i. The Privacy Statement must include a statement explaining that the Site is a participant in the TRUSTe Program, and is using the TRUSTe Mark(s) under license from TRUSTe pursuant to the requirements of the TRUSTe program, and that all rights in the TRUSTe Mark(s) belong to TRUSTe. This statement shall include a full description of how users of the Site can contact Licensee as well as a description of how to contact TRUSTe to express concerns regarding Licensee's Privacy Statement.	1
3. Contractual or other means used to assure comparable protection of information transferred to third parties for processing		0
Identifying Purposes Principle: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.		
4. Specify purposes to data subject at or before time of collection	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program (as amended by **Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0, Part 5)** A. Licensee's Privacy Statement shall be made available to users of the Site ("Users") prior to or at the time Personally Identifiable Information or Third	1

PIPA	TRUSTe	Pts
	Party Personally Identifiable Information is collected. The Privacy Statement shall disclose to Users the Site's information use and collection practices, including each of the following: iii. How Personally Identifiable Information and/or Third Party Personally Identifiable Information collected through the Site may be used and the purposes of such use. **TRUSTe Site Coordinator's Guide** **Implementation** 7 b) The trustmark (Final Mark) should be placed on the homepage and at the point of data collection and must link directly to the approved privacy statement. The trustmark cannot be altered in any way. If for some reason it is not possible to place the trustmark on the site, then you may request that a "Privacy Statement" text link be used. Again, the text link must be linked directly to your privacy statement.	
Consent Principle: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.		
5. Knowledge and consent of data subject	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program A. Privacy Statement. Licensee's Privacy Statement shall be made available to users of the Site ("Users") prior to or at the time Personally Identifiable Information or Third Party Personally Identifiable Information is collected. The Privacy Statement shall disclose to Users the Site's information use and collection practices, including each of the following: i. What Personally Identifiable Information pertaining to Users and/or Third Party Personally Identifiable Information is collected through the Site; ii. The identity of the organization (including name, address, phone number, and e-mail address) collecting the Personally Identifiable Information and/or Third Party Personally Identifiable Information through the Site; iii. How Personally Identifiable Information and/or Third Party Personally Identifiable Information collected through the Site may be used; iv. With whom Personally Identifiable Information and/or Third Party Personally Identifiable Information collected through the Site may be shared, if at all; v. What choices are available to the User of the Site regarding collection, use, disclosure, and distribution of Personally Identifiable Information; **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.1 Information Disclosure Explain up front what Personally Identifiable Information (PII) is being gathered, who is gathering the information, what the information is used for,	1

PIPA	TRUSTe	Pts
	and with whom the information is being shared. After reading your statement, users should have no questions about *why* they are giving you their name, email address, company name, and other information, as this should be explained to them clearly in the privacy statement. 3.1.1 Collection and Use of Information Begin by explaining what information you collect through your web site and how it is used. Address all sections/pages where information is collected (this includes affiliate sign-up pages, feedback forms, and contact us forms). Disclose how you collect information explicitly, such as via registration forms, order forms, and contests. 3.1.3 Sharing of Information Next, you must disclose who you share the information with, if anyone. Sharing with subsidiaries and other companies is considered third party sharing and must also be disclosed in your privacy statement. If you do not share the information with any third parties, disclose this as well. **TRUSTe Program Principles** At a minimum, your privacy statement needs to disclose: The choices available to users regarding collection, use, and distribution of their information: You must offer users an opportunity to opt-out of internal secondary uses as well as third party distribution for secondary uses.	
6. Product or service cannot be denied if data subject refuses to divulge information beyond that required for specified, legitimate purpose	**TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.1.1 Mandatory or Optional Information State in your privacy statement, or clearly mark on the web site, whether the information being requested is mandatory or optional. What are the consequences if the user does not give the information? Will the user still be allowed to participate? Will the user still be given access the site/service? Explain the benefits of disclosing any information considered "optional."	1
7. Data subject may withdraw consent	**TRUSTe License Agreement Version 6** **Schedule A** 3. Minimum Requirements of the TRUSTe Program B. Privacy Practices. i. (as amended by **Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0, Part 6)** Choice. Licensee shall offer the user the opportunity to exercise affirmative choice (e.g. to "Opt Out" as defined below) before Personally Identifiable Information collected through the Site may be (1) used when such use is unrelated to the primary purpose for which the information was collected; or (2) disclosed or distributed to third parties, unless such disclosure or distribution is made to a third party that is acting as an agent of Licensee to perform task(s) on behalf of and under the instructions of Licensee. The scope of uses deemed "related" shall be defined in the Privacy Statement. At a minimum, if Licensee states in its Privacy Statement that it provides Personally	1

PIPA	TRUSTe	Pts
	Identifiable Information to third parties and such use, disclosure or distribution is unrelated to the purpose for which the information was collected, users must always be given the opportunity to opt out of such use, disclosure or distribution. "Opt Out" means to notify the Site operator that they do not wish to have their Personally Identifiable Information used, disclosed or distributed in a manner that is unrelated to the primary purpose for which the information was collected, whereupon the Site operator shall ensure that the user's choice is complied with. Such Opt-Out opportunity shall not in any way limit the use, disclosure or distribution of Personally Identifiable Information to the extent such use, disclosure or distribution is required by law, court order, or other valid legal process. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.2 Choice/Opt-Out or Opt-In The privacy statement needs to explain what choices are available to the user regarding the collection, use, and distribution of the information. Provide visitors with a mechanism to opt-out of having Personally Identifiable Information used by the site for any secondary purposes or disclosed to third parties. Your site needs to provide users the ability and mechanism to opt-in or opt-out of having their information shared with any third parties for which it is not necessary to carry out the service. Also, you must present an opportunity to opt-out for such secondary purpose of use to your user before the site sends the first communication. The privacy statement needs to let users know how they are able to opt-out of receiving secondary communications from the site. **TRUSTe Site Coordinator's Guide** **Recommended Guidelines for a Comprehensive Privacy Statement** 4.4 Provide consumers with a mechanism to delete/deactivate personal information from the site's database upon request. You may want to set the user's expectation by specifying the time frame for the delete/deactivation to take place. "Deactivating" refers to the process by which a database manager may delete Personally Identifiable Information, upon request, from its database. Because of backups, and records of deletions, it may be impossible to delete a consumer's entry without some residual information. An individual who requests to have Personally Identifiable Information deactivated will be functionally deleted, and a company may not sell, transfer, or use Personally Identifiable Information relating to that individual in any way.	
Limiting Collection Principle: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.		
8. Data collection limited to that necessary for identified purposes	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program B. Privacy Practices vi. Use of Personally Identifiable Information and/or Third Party Personally Identifiable Information. Licensee shall treat all Personally Identifiable Information and/or Third Party Personally Identifiable Information gathered	1

PIPA	TRUSTe	Pts
	on the Site in accordance with Licensee's Privacy Statement(s) in effect at the time of collection. viii. Limit on Use of Third Party Personally Identifiable Information. Third Party Personally Identifiable Information collected through the Site may be used solely by Licensee or by other parties when necessary to facilitate the completion of the transaction that is the primary purpose for which the information was collected.	
9. Data collection only by lawful and fair means		0
Limiting Use, Disclosure and Retention Principle: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.		
10. Use and disclose in accordance with specified purposes	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program B. Privacy Practices v. Displaying Personally Identifiable Information and/or Third Party Personally Identifiable Information. Licensee shall not make Personally Identifiable Information and/or Third Party Personally Identifiable Information available to the general public in any form (including but not limited to on-line directories and customer lists) without the prior written or electronic consent of the individual identified. vi. Use of Personally Identifiable Information and/or Third Party Personally Identifiable Information. Licensee shall treat all Personally Identifiable Information and/or Third Party Personally Identifiable Information gathered on the Site in accordance with Licensee's Privacy Statement(s) in effect at the time of collection. viii. Limit on Use of Third Party Personally Identifiable Information. Third Party Personally Identifiable Information collected through the Site may be used solely by Licensee or by other parties when necessary to facilitate the completion of the transaction that is the primary purpose for which the information was collected.	1
11. Except with data subject consent or by authority of law	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program A. Privacy Statement. Licensee's Privacy Statement shall be made available to users of the Site ("Users") prior to or at the time Personally Identifiable Information or Third Party Personally Identifiable Information is collected. The Privacy Statement shall disclose to Users the Site's information use and collection practices, including each of the following: viii. The fact that Personally Identifiable Information and/or Third Party Personally Identifiable Information provided to Licensee is subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders.	1

PIPA	TRUSTe	Pts
	B. Privacy Practices v. Displaying Personally Identifiable Information and/or Third Party Personally Identifiable Information. Licensee shall not make Personally Identifiable Information and/or Third Party Personally Identifiable Information available to the general public in any form (including but not limited to on-line directories and customer lists) without the prior written or electronic consent of the individual identified, except that this paragraph shall not prevent or restrict Licensee from (i) distributing information that already is publicly available, including but not limited to information available in public telephone directories, classified ads, newspaper reports, publications, and the like; (ii) providing information as required by law, court order, or other valid legal process; or (iii) displaying information in an on-line bulletin board, chat room, news group, or other public forum, where the information being displayed was placed there by a user or other third party. A Licensee operating an on-line directory, or other similar service, must provide a process whereby individuals may Opt Out whereupon the Site operator shall remove such Personally Identifiable Information from such on-line directory-type service. The parties agree that if Licensee's Site(s) provide links to other sites, which make available such directories, or lists, such links shall not be a violation of this provision. vi. Use of Personally Identifiable Information and/or Third Party Personally Identifiable Information. Licensee shall treat all Personally Identifiable Information and/or Third Party Personally Identifiable Information gathered on the Site in accordance with Licensee's Privacy Statement(s) in effect at the time of collection. If Licensee wishes to materially change its Privacy Statement(s), or change its use of data, Licensee shall notify TRUSTe of the changes and shall take commercially reasonable measures to obtain the consent from the user to whom it pertains, such as obtaining written or electronic consent of the user. Alternatively, with prior written approval by TRUSTe, which approval should not be unreasonably withheld or delayed, Licensee may post prominent notices on the Site about the change of such use or policy and leave such notices posted for at least thirty (30) business days prior to implementation of the new use and a description of how to notify Licensee to prevent such use. The Privacy Statement shall set forth the notification procedures (with respect to a material change in the Privacy Statement(s), or use of Personally Identifiable Information and/or Third Party Personally Identifiable Information) which will be employed by Licensee prior to a material change in the Privacy Statement(s). Licensees making material changes to their privacy statements may be subject to a revision fee. viii. Limit on Use of Third Party Personally Identifiable Information. Third Party Personally Identifiable Information collected through the Site may be used solely by Licensee or by other parties when necessary to facilitate the completion of the transaction that is the primary purpose for which the information was collected. Third Party Personally Identifiable Information collected through the Site may not be otherwise used or disclosed or distributed to other parties unless Licensee first provides the person identified by the Third Party Personally Identifiable Information a reasonable means for the third party to notify the Site Operator that they do not wish to have their Third Party Personally Identifiable Information used, disclosed or distributed	

PIPA	TRUSTe	Pts
	(e.g. Opt Out), whereupon the Site operator shall ensure that the identified person's choice is complied with.	
12. Data retained only as long as necessary for specified purposes		0
13. New uses of personal information shall be documented	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements:** 3. Minimum Requirements of the TRUSTe Program B. Privacy Practices. vi. Use of Personally Identifiable Information and/or Third Party Personally Identifiable Information. Licensee shall treat all Personally Identifiable Information and/or Third Party Personally Identifiable Information gathered on the Site in accordance with Licensee's Privacy Statement(s) in effect at the time of collection. If Licensee wishes to materially change its Privacy Statement(s), or change its use of data, Licensee shall notify TRUSTe of the changes and shall take commercially reasonable measures to obtain the consent from the user to whom it pertains, such as obtaining written or electronic consent of the user. Alternatively, with prior written approval by TRUSTe, which approval should not be unreasonably withheld or delayed, Licensee may post prominent notices on the Site about the change of such use or policy and leave such notices posted for at least thirty (30) business days prior to implementation of the new use and a description of how to notify Licensee to prevent such use. The Privacy Statement shall set forth the notification procedures (with respect to a material change in the Privacy Statement(s), or use of Personally Identifiable Information and/or Third Party Personally Identifiable Information) which will be employed by Licensee prior to a material change in the Privacy Statement(s). Licensees making material changes to their privacy statements may be subject to a revision fee. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.5 Notification of Changes Let users know how the site will notify them if there is a change in privacy practices. Currently, we require licensees to obtain written or active email consent from the user if the company is going to be using the information collected from the user in a manner different from that stated at the time of collection. For some business models, it may be acceptable to obtain the user's consent by posting notice on the site with prior approval by TRUSTe. The privacy statement needs to let users know how the site will notify them of any changes in the use of their personally identifiable information. Note that without user approval, your policy must be to handle information under which policy it was collected.	1

PIPA	TRUSTe	Pts
Accuracy Principle: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.		
14. Accurate, complete and up-to-date	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program (as amended by **Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0, Part 7)** B.iii. Data Quality and Access Licensee shall take reasonable steps when collecting, creating, maintaining, using, disclosing or distributing Personally Identifiable Information and/or Third Party Personally Identifiable Information, to assure that the data are accurate, complete and timely for the purposes for which they are to be used. **TRUSTe Program Principles** At a minimum, your privacy statement needs to disclose: How users can update or correct inaccuracies in their pertinent information: Appropriate measures shall be taken to ensure that personal information collected online is accurate, complete, and timely, and that easy-to-use mechanisms are in place for users to verify that inaccuracies have been corrected.	1
Safeguards Principle: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.		
15. Appropriate security safeguards	**TRUSTe License Agreement Version 6** **Schedule A** 3. Minimum Requirements of the TRUSTe Program B. Privacy Practices. ii. Security Licensee must implement reasonable procedures to protect Personally Identifiable Information and/or Third Party Personally Identifiable Information within its control that results in unauthorized distribution, use, or misuse; or unauthorized access, disclosure, or alteration.* (sic) If Licensee collects, uses, discloses or distributes sensitive information, such as credit card numbers or social security numbers, it shall utilize appropriate commercially reasonable practices, such as encryption, to protect information transmitted over the Internet. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.4 Security If your Web site collects personally identifiable information, you must have reasonable security mechanisms to protect the data collected. Include in the privacy statement a general statement about the procedures that are in place to protect the loss, misuse, or alteration of information collected. At a minimum, questions that should be considered are:	1

* There seems to be some kind of drafting error here. The first sentence stops making sense after the word "that." The intent of the section would probably be properly captured if the words "that results in" were replaced with "against."

PIPA	TRUSTe	Pts
	a) How do you make employees aware of your security policy and practices? b) Is access to data limited? How do your employees obtain access? Via password, token, smart card, etc.? c) Do you periodically review your web security? How often? d) If sensitive information, such as credit card numbers or social security numbers, is collected, used, or disseminated, is there a commercially accepted protocol, such as encryption, in place to protect information sent over the Internet?	
Openness Principle: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.		
16. Ready access for data subject to policies and practices	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 2.F. Privacy Statement(s). Licensee shall maintain and abide by a privacy statement that is written by Licensee, approved by TRUSTe, that, reflects Licensee's information use policies, and is easily accessible at Licensee's Site ("Privacy Statement"). **TRUSTe Site Coordinator's Guide** **Developing a Privacy Statement** To meet TRUSTe's guidelines, a privacy statement must at a minimum disclose the following: • What personally identifiable information is collected • What organization is collecting the information • How the information is used • With whom the information may be shared • What choices are available to users regarding collection, use and distribution of the information • What kind of security procedures are in place to protect against the loss, misuse or alteration of information under the company's control • How users can correct any inaccuracies in the information. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.1 Information Disclosure You must explain and summarize your general information-gathering practices.	1
17. Policies and practices available in generally understandable form	**TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.6 Readability The privacy statement must be easy to read and understand. Use language that will not confuse or frustrate users. We suggest writing at an eighth grade level without any legal jargon.	1

PIPA	TRUSTe	Pts
18. Ready access to description of type of personal information held, including general account of its use	**TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.1 Information Disclosure Explain up front what Personally Identifiable Information (PII) is being gathered, who is gathering the information, what the information is used for, and with whom the information is being shared. After reading your statement, users should have no questions about why they are giving you their name, email address, company name, and other information, as this should be explained to them clearly in the privacy statement.	1
19. Ready access to description of what personal information made available to related organizations	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 2.F.ii. The Privacy Statement must identify anyone who collects or maintains personal information from or about the users of the Site, or has an interest in the information collected, or on whose behalf such information is collected or maintained. If the Site is co-owned, all co-owners must be governed by the terms of the Privacy Statement. If the Site is not co-owned, but is coordinated with another site in such a way that users or visitors would reasonably expect that the two sites are part of one continuous site, each coordinated web page must identify who is collecting information and provide a link to the Privacy Statement. In situations involving co-branded or partner sites, the Privacy Statement must indicate who is collecting information on the Site and to whom the Privacy Statement applies. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.1.3 Sharing of Information Next, you must disclose who you share the information with, if anyone. Sharing with subsidiaries and other companies is considered third party sharing and must also be disclosed in your privacy statement. If you do not share the information with any third parties, disclose this as well. Often, it is just as informative to know what the web site does *not* do with the information as to know what the web site *does* with it. Furthermore, if you have intermediary relationships such as credit card processing and shipping companies, you need to disclose these relationships as well. Finally, you must state your policy regarding the release of information to law enforcement under court order or subpoena.	1
Individual Access Principle: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.		
20. Data subject informed of existence, use, and disclosure of personal information	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program A. Privacy Statement ... The Privacy Statement shall disclose to Users the Site's information use and collection practices, including each of the following: vii. Whether Users of the Site are offered access to their Personally Identifiable Information and how they may have inaccuracies corrected.	1

PIPA	TRUSTe	Pts
21. Data subject can access personal information	**Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0** 7. iii. a. Except as provided in section 3.B.iii.b, Licensee must permit any user requesting access to Personally Identifiable Information collected and stored about that user ("Requesting User") to access such information upon receipt of sufficient information to confirm the Requesting User's identity.	1
22. Personally identifying information disclosed to gain access to information shall be used for no other purpose		0
23. Data communicated within 30 days and at a minimal or no cost to the individual	**Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0** 7. iii. a. Except as provided in section 3.B.iii.b, if Licensee does not provide a Requesting User the requested access within thirty (30) calendar days of the Requesting User's request, Licensee must provide the Requesting User with a timeline establishing when the requested access will be provided.	0.5
24. Requested information must be in form that is generally understandable	**Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0** 7. iii. a. The Personally Identifiable Information must be provided to users in a readily intelligible form.	1
25. Reasons for denying access set out along with any available recourse	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program (as amended by **Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0, Part 7)** B.iii. Data Quality and Access c. If Licensee denies access to Personally Identifiable Information pursuant to section 3.B.iii.b, Licensee must provide the Requesting User with an explanation of why access was denied, and with contact information for further inquiries regarding the denial of access.	1
26. Ability to challenge and amend	**TRUSTe License Agreement Version 6** **Schedule A: Program Requirements** 3. Minimum Requirements of the TRUSTe Program (as amended by **Addendum to the TRUSTe License Agreement, Program Requirements and Self-Assessment Sheet Version 1.0, Part 7)** B.iii Data Quality and Access Licensee must implement reasonable and appropriate processes or mechanisms to allow users to correct, amend or delete inaccuracies in Personally Identifiable Information collected through the Site. These processes or mechanisms must be simple and easy to use, and shall confirm to users that inaccuracies have been corrected, amended or deleted. Such a mechanism could	1

PIPA	TRUSTe	Pts
	include, but is not limited to, accepting written or e-mailed requests for information, and having an employee copy the relevant information and send the information to the requesting individual. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.3 Correct/Update Users must be provided with a mechanism to correct, access and update pertinent Personally Identifiable Information obtained through the site. Mechanisms include online, email, telephone, postal mail, etc. This will help assure that the information you collect is accurate and up to date. The privacy statement needs to state how a user can correct, access, and update their personal information. **TRUSTe Program Principles** At a minimum, your privacy statement needs to disclose: How users can update or correct inaccuracies in their pertinent information: Appropriate measures shall be taken to ensure that personal information collected online is accurate, complete, and timely, and that easy-to-use mechanisms are in place for users to verify that inaccuracies have been corrected.	
27. Where appropriate, amended information passed on to third parties with access		0
28. Substance of unresolved challenges to information shall be recorded		0
29. Where appropriate, existence of unresolved challenges transmitted to third parties with access		0
Challenging Compliance Principle: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.		
30. Data subject can challenge compliance with principles	**TRUSTe License Agreement Version 6.0** **Schedule A: Program Requirements** 4. Reviews. ... To comply with this s. 4, Licensee agrees to: B. Be subject to an on-site compliance review in response to non-frivolous complaints from a user of the Site or TRUSTe that Licensee (i) has failed to implement and adhere to the policies set forth in Licensee's Privacy Statement; or (ii) has failed to adhere to the Program Requirements. If Licensee has	1

PIPA	TRUSTe	Pts
	materially breached this Agreement, Licensee agrees to reimburse TRUSTe for the reasonable cost of any such review and promptly rectify the practice to TRUSTe's reasonable satisfaction. 5. User Complaints. Licensee shall provide users with reasonable, appropriate, simple and effective means to submit complaints and express concerns regarding Licensee's privacy practices. Licensee shall respond to all reasonable user submissions in a timely fashion, not to exceed ten (10) business days. **TRUSTe Site Coordinator's Guide** **TRUSTe's Required Guidelines** 3.8 TRUSTe Opening Paragraph You may include the TRUSTe opening paragraph in your privacy statement. If you chose not implement the opening paragraph, at a minimum you must include a statement indicating: a) That you are a TRUSTe licensee. b) How users can contact you or TRUSTe should they feel that the web site is not abiding by its posted privacy policy.	
31. Justified complaints addressed by appropriate measures, including, if necessary, amending policies and practices	**TRUSTe License Agreement Version 6.0** **Schedule A: Program Requirements** 5. User Complaints. ... Licensee shall respond to all reasonable user submissions in a timely fashion, not to exceed ten (10) business days.	0.5
	TOTAL	23

APPENDIX 6: WEBTRUST

*Principles from Schedule 1 of the *PIPA*; criteria 1-31 are author's own analysis of the principles; WebTrust listings, see *supra* note 208 of article.

PIPA	WebTrust	Pts
Accountability Principle: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.		
1. Data controller(s) accountable for compliance with principles	**WebTrust Privacy Criteria** **Policies, Goals and Objectives** B.3. Accountability for the entity's privacy and related security policies has been assigned.	1
2. Data controller(s) identity available on request	**WebTrust Privacy Criteria** **Disclosures** A.4. The entity discloses information to enable customers to contact it for questions or support.	1
3. Contractual or other means used to assure comparable protection of information transferred to third parties for processing	**WebTrust Privacy Criteria** **Procedures and Technology Tools** **Privacy Specific Criteria** C.12. The entity has procedures to obtain assurance or a representation that the adequacy of information protection and privacy policies of third parties to whom information is transferred, and upon which the entity relies, is in conformity with the entity's disclosed privacy practices.	1
Identifying Purposes Principle: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.		
4. Specify purposes to data subject at or before time of collection	**WebTrust Privacy Criteria** **Disclosures** A.1.1. The entity discloses on its web site the specific kinds and sources of information being collected and maintained, the use of that information, and possible third party distribution of that information.	1
Consent Principle: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.		
5. Knowledge and consent of data subject	**WebTrust Privacy Criteria** **Disclosures** A.1.1. The entity discloses on its web site the specific kinds and sources of information being collected and maintained, the use of that information, and possible third party distribution of that information. A.1.2. The entity discloses on its web site choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt-out of such use, by either not providing such information or denying its distribution to parties not involved with the transaction. A.1.3. The entity discloses on its web site sensitive information needed for the e-commerce transaction. Individuals must **opt-in** before this information is gathered and transmitted.	1

PIPA	WebTrust	Pts
	A.2. If the web site uses cookies or other tracking methods (for example, web bugs and middleware), the entity discloses how they are used. If the customer refuses cookies, the consequences, if any, of such refusal are disclosed. **Policies Goals and Objectives** B.1. The entity's policies regarding the protection of personal information include, but are not limited to, the following items: • Notice to the customer regarding the information collected • Choice to the customer regarding the type(s) of information gathered and any options the customer has regarding the collection of this information.	
6. Product or service cannot be denied if data subject refuses to divulge information beyond that required for specified, legitimate purpose	**WebTrust Privacy Criteria** **Disclosures** A.1.4. The entity discloses on its web site consequences, if any, of an individual's refusal to provide information or of an individual's decision to opt-out (or not opt-in) of a particular use of such information.	1
7. Data subject may withdraw consent	**WebTrust Privacy Criteria** **Disclosures** A.1.2. The entity discloses on its web site choices regarding how personal information collected from an individual online may be used and/or distributed. Individuals are given the opportunity to opt-out of such use, by either not providing such information or denying its distribution to parties not involved with the transaction.	1
Limiting Collection Principle: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.		
8. Data collection limited to that necessary for identified purposes	**WebTrust Privacy Criteria** **Monitoring and Performance Measures** D.2. The entity has procedures in place to keep its disclosed privacy and related security policies current with laws and regulations and to monitor adherence to its current privacy and security policy practices. **WebTrust Privacy Criteria** **Policies, Goals and Objectives** B.5. The entity's privacy and related security policies are consistent with disclosed privacy practices and applicable laws and regulations.	1
9. Data collection only by lawful and fair means	**WebTrust Privacy Criteria** **Disclosures** A.6. The entity discloses any additional privacy practices needed to comply with applicable laws or regulations or any self-regulatory programs in which the entity participates.	0.5

PIPA	WebTrust	Pts
	Policies, Goals and Objectives B.5. The entity's privacy and related security policies are consistent with disclosed privacy practices and applicable laws and regulations. **Monitoring and Performance Measures** D.2. The entity has procedures in place to keep its disclosed privacy and related security policies current with laws and regulations and to monitor adherence to its current privacy and security policy practices.	
Limiting Use, Disclosure, and Retention Principle: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.		
10. Use and disclose in accordance with specified purposes	**WebTrust Privacy Criteria** **Monitoring and Performance Measures** D.2. The entity has procedures in place to keep its disclosed privacy and related security policies current with laws and regulations and to monitor adherence to its current privacy and security policy practices. **WebTrust Privacy Criteria** **Policies, Goals and Objectives** B.5. The entity's privacy and related security policies are consistent with disclosed privacy practices and applicable laws and regulations.	1
11. Except with data subject consent or by authority of law	**WebTrust Privacy Criteria** **Procedures and Technology Tools** **Privacy Specific Criteria** C.9. The entity has procedures to ensure private information obtained as a result of electronic commerce is only disclosed to parties essential to the transaction unless customers are clearly notified prior to providing such information. If the customer was not clearly notified when he or she submitted the information, customer permission is obtained before such information is released to third parties. C.14. In the event that a disclosed privacy policy is changed or deleted to be *less* restrictive, the entity has procedures to protect personal information in accordance with the privacy policies in place when such information was collected. Clear and conspicuous customer notification and choice are required to allow the entity to follow the new privacy policy with respect to their personal information.	0.5
12. Data retained only as long as necessary for specified purposes		0
13. New uses of personal information shall be documented	**WebTrust Privacy Criteria** **Disclosures** A.7. The entity discloses changes or updates to its privacy practices.	1

PIPA	WebTrust	Pts
Accuracy Principle: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.		
14. Accurate, complete, and up-to-date	**WebTrust Privacy Criteria** **Procedures and Technology Tools** **Security Criteria That Relate to Privacy** C.3. The entity has procedures to allow users to change, update, or delete their own user profile. **Procedures and Technology Tools** **Privacy Specific Criteria** C.11 The entity has procedures for personally identifiable information collected, created, or maintained by it to subject the information to reasonable edit and validation checks as it is collected.	0.5
Safeguards Principle: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.		
15. Appropriate security safeguards	**WebTrust Privacy Criteria** **Procedures and Technology Tools** **Security Criteria That Relate to Privacy** C.1. The entity has appropriate security procedures to establish new users. C.2. The entity has procedures to identify and authenticate authorized users. C.3. The entity has procedures to allow users to change, update, or delete their own user profile. C.4. The entity has procedures to limit remote access to the internal network to only authorized personnel. C.5. The entity has procedures to prevent customers, groups of individuals, or other entities from accessing other than their own private or sensitive information. C.6. The entity has procedures to limit access to personally identifiable information to only authorized employees based upon their assigned roles and responsibilities. C.7. The entity utilizes a minimum of 128-bit encryption to protect transmission of user authentication, verification, and sensitive or private information that is passed over the Internet from unintended recipients. C.8. The entity has procedures to maintain system configurations that minimize security exposures potentially affecting private or sensitive information.	1
Openness Principle: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.		
16. Ready access for data subject to policies and practices	**WebTrust Privacy Criteria** **Disclosures** A.1. The entity discloses on its web site its information privacy practices.	1

PIPA	WebTrust	Pts
17. Policies and practices available in generally understandable form		0
18. Ready access to description of type of personal information held, including general account of its use	**WebTrust Privacy Criteria** **Disclosures** A.1.1. The entity discloses on its web site the specific kinds and sources of information being collected and maintained, the use of that information, and possible third party distribution of that information.	1
19. Ready access to description of what personal information made available to related organizations	**WebTrust Privacy Criteria** **Disclosures** A.1.1. The entity discloses on its web site the specific kinds and sources of information being collected and maintained, the use of that information, and possible third party distribution of that information.	1
Individual Access Principle: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.		
20. Data subject informed of existence, use, and disclosure of personal information	**WebTrust Privacy Criteria** **Disclosures** A.1.1. The entity discloses on its web site the specific kinds and sources of information being collected and maintained, the use of that information, and possible third party distribution of that information. A.1.5. The entity discloses on its web site how personal information collected can be reviewed and, if necessary, corrected or removed.	1
21. Data subject can access personal information	**WebTrust Privacy Criteria** **Disclosures** A.1.5. The entity discloses on its web site how personal information collected can be reviewed and, if necessary, corrected or removed.	1
22. Personally identifying information disclosed to gain access to information shall be used for no other purpose		0
23. Data communicated within 30 days and at a minimal or no cost to the individual		0
24. Requested information must be in form that is generally understandable		0

PIPA	WebTrust	Pts
25. Reasons for denying access set out along with any available recourse		0
26. Ability to challenge and amend	**WebTrust Privacy Criteria** **Disclosures** A.1.5. The entity discloses on its web site how personal information collected can be reviewed and, if necessary, corrected or removed. **Policies Goals and Objectives** B.1. The entity's policies regarding the protection of personal information include, but are not limited to, the following items: • Access by the customer to his or her private information for update and corrective purposes. **Procedures and Technology Tools** **Security Criteria That Relate to Privacy** C.3. The entity has procedures to allow users to change, update, or delete their own user profile.	1
27. Where appropriate, amended information passed on to third parties with access		0
28. Substance of unresolved challenges to information shall be recorded		0
29. Where appropriate, existence of unresolved challenges transmitted to third parties with access		0
Challenging Compliance Principle: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.		
30. Data subject can challenge compliance with principles	**WebTrust Privacy Criteria** **Disclosures** A.5. The entity discloses its procedures for consumer recourse for issues regarding privacy that are not resolved by the entity. These complaints may relate to collection, use and distribution of private information, and the consequences for failure to resolve such complaints. This resolution process should have the following attributes:	1

PIPA	WebTrust	Pts
	• Management's commitment to use a specified third party dispute resolution service or other process mandated by regulatory bodies in the event the customer is not satisfied with the entity's proposed resolution of such a complaint together with a commitment from such third party to handle such unresolved complaints. Procedures to be followed in resolving such complaints, first with the entity and, if necessary, with the designated third party. • What use or other action will be taken with respect to the private information, which is the subject of the complaint, until the complaint is satisfactorily resolved.	
31. Justified complaints addressed by appropriate measures, including, if necessary, amending policies and practices		0
	TOTAL	19.5