The Evolution of Consumer Privacy Law: How Privacy by Design can Benefit from Insights in Commercial Law and Standardization

Muharem Kianieff[*]

This article considers the effectiveness of the present privacy regimes in North America as it relates to the protection of consumer information that is gathered in the ordinary course of business. It is argued that the present moves towards a Privacy by Design approach shows great potential and can gain valuable insights from established doctrines in commercial and consumer protection law. Moreover, it is proposed that the aims of such an approach can be achieved by deeming personal information and behavioral data to be the property of the individual that it pertains to. It is then suggested that a regulatory framework be enacted whereby consumers could grant licenses to entities to use this information based upon predefined standard terms that would limit the scope and transferability of the information. It is argued that this will empower consumers and help to reduce the temptation for entities to act in a manner that hinders consumer expectations.

INTRODUCTION

> *That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth grows to meet the needs of society.*[1]

With these words, Warren and Brandeis began their famous article "The Right to Privacy" in 1890. What was true then is still true today, namely that economic and social changes force the law to keep pace with new innovations to maintain an appropriate balance between fostering innovation and ensuring that the fundamental rights of individuals are not compromised by new technological developments. One such challenge to individual privacy that has come to the forefront in the last twenty years has been through technological advances that have allowed informa-

---

* Assistant Professor, University of Windsor, Faculty of Law.

This article was made possible through a generous grant of the Law Foundation of Ontario. I would like to express my gratitude to Professor Leonard I. Rotman for his suggestions and support. I also wish to thank Professor Myra Tawfik, Professor William Conklin, Professor Laverne Jacobs, Jason Bird and an anonymous reviewer for their valuable thoughts and comments. For research assistance, I am grateful to Windsor Law student Jonah Moses. Last but not least, I would also like to thank Professor Michael Deturbide for his editorial assistance.

1 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 (5) Harv L Rev 193.

tion to be gathered, stored, processed and transmitted at a pace once thought unimaginable. As information technology reached greater heights, privacy has remained an area of concern to consumers despite reassurances and changing approaches that are designed to allay consumer fears. Since some time has passed and consumers are now approaching the Internet with a greater familiarity, it may be fitting to evaluate some of the responses to consumer privacy concerns that have been developed recently and consider new areas of research and potential solutions to lingering challenges.

Many of the privacy implications that result from the evolution of new technologies do not stem from information that is gathered illicitly, although this in itself leads to consumer concerns with respect to the security of their personal details that are held by various commercial entities. However, one area that does not receive as much media attention as illicit attacks are instances where entities utilize information that is legitimately collected for uses authorized by a consumer in one context that is then put to a use that a consumer may not have been aware of at the time that they gave consent to its collection, or information is put to a use not originally contemplated by the consumer when it was legitimately collected.

The challenges posed by increased information processing technology force us to reconsider what role the law ought to play in enhancing individual privacy rights. This is true even if it stifles the flow of information or limits technology's potential to develop new products and bring greater convenience if it simultaneously allows greater access to our personal details, tastes, spending habits and behavioral traits. While this technology is new, the fundamental paradigm that is a right to be left alone, as posited by Warren and Brandeis,[2] is not.

This paper considers the effectiveness of various approaches that have been adopted in North America as they relate to consumer information gathered in the ordinary course of business and that may be put to uses not authorized or envisaged by the consumer at the time that the information was obtained. In particular, many of the problems currently facing consumers in this area are similar to those found in other areas of law particularly in the commercial law and or consumer protection context. As such, innovations through the proposed Privacy by Design framework may benefit from adapting regulatory approaches developed in other areas of law and public policy. In particular, it will be suggested that all information pertaining to a consumer ought to remain the property of that individual at all times. Any interactions with this data in the commercial sector should only be allowed after the consumer has granted these entities a license to deal with their information that is immediately revocable upon the insolvency of the commercial entity or upon any unauthorized use. Moreover, it will be argued that licenses should be granted based upon pre-defined privacy ratings standards (similar to those used for motion pictures or television programs) that would bind both the initial gatherer of the information and any subsequent parties that may come into contact with it. These licenses would allow consumers to specify the types of permitted uses their information may be put to and allow for some flexibility for consumers to decide what type of license they wish to grant.

Part I will discuss some of the privacy issues in the private realm that have

---

2 *Ibid.*

become prominent in privacy debates from the mid 1990's to the 2010's in North America. Part II will consider some of the empirical studies that have been conducted since that time. Particular attention will be paid to studies that describe how effective some of the earlier methods of regulation have fared. Part III will discuss some of the newer views on privacy regulation that have emerged over the past two years, and evaluate some proposals that regulators may look to as they move to meet consumer expectations.

I. PRIVATE SPHERE PRIVACY REGULATION IN NORTH AMERICA

(a) How the Private Sector Uses Personal Data

The open nature of the Internet coincided with other advances in technology that made electronic commerce a more attractive proposition for business. In particular, advances in database technologies and falling costs for data storage and analysis have also allowed business to develop new models for use in the digital age.[3] With the advent of computers many businesses found it advantageous to use databases as a means of supporting their internal operations particularly in support of marketing and management decision making.[4]

Winn and Wrathall define databases as a collection of data that is organized so that its contents can be easily accessed, managed and updated.[5] Relational databases are those in which data can be accessed in a number of different ways without having to reorganize the database. It is now not uncommon to see many companies operating data warehouses which serve as central repositories for all or significant parts of the data that a company and its affiliates may collect.[6] The technological development of cookies, clickstream and TGI form an integral part of data warehousing. Once the data is collected, a company may then engage in what is known as "data mining."

Data mining involves analyzing data in order to discover previously undiscovered relationships.[7] Using these tools of analysis, it is possible to establish associations between facts that were not known to have any correlation. It can also establish the chronological sequence of events, classify data according to newly recognized patterns such as customer profiles, arrange data into groups not previously known and make forecasts based upon newly discovered patterns that aid prediction.[8] Data mining, then, is crucial to being able to make sense of the data that is collected from various sources in order to derive conclusions from the data

---

3 Jane Kaufman Winn & James R Wrathall, "Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Consumer Data", online: Southern Methodist University <http://www.law.washington.edu/Directory/docs/Winn/Who%20Owns%20the%20Customer.htm> at 13.

4 *Ibid.*

5 *Ibid.*

6 *Ibid* citing Vivek R Gupta, "System Services Corporation, An Introduction to Data Warehousing", online: System Services Corp <http://www.sserve.com/dwintro.asp>.

7 *Ibid.*

8 *Ibid* citing Gupta, *supra* note 6.

itself.

The business implications that result from data mining are twofold. First is the fact that the information that is collected may be of value not only to the entity that has collected it but to other entities as well. Companies can avail themselves of lucrative opportunities to sell or rent out the information that they have compiled.[9] It is estimated that the personal information about one individual alone may be worth as much as $277 U.S.[10] Also valuable is the ability of the information to shore up sales of their products and maximize the potential of their advertising / marketing. Data mining can allow product developers to determine which segments of the population their product appeals to, analyze the motivations of consumers and forecast which techniques are likely to increase revenue. It is particularly useful for companies that sell a large variety of products.[11]

Advances in the past number of years have provided greater abilities to store even vaster amounts of data than was thought possible even five years ago.[12] This has compounded the storage capabilities that made data warehousing and mining even more of an attractive proposition for those that are interesting in acquiring behavioral data. Indeed, one of the unintended consequences of these technological advances is that it now costs more to delete the data off of these storage devices than it is to retain it.[13] Thus the economics that has worked in favor of retaining data and providing increasing returns to scale by extrapolating behavioral information from it is now a disincentive to safely disposing of this data once it has been put to its intended use. Regardless of this fact, recent events (described below) would seem to suggest that increasing returns to scale in data retention and analysis have made a market based approach less desirable as entities have shown themselves unwilling or unable to mitigate the effects (either intended or unintended) of unauthorized uses of consumer data.

(b) Privacy Regulation in the Mid-1990's

As the Internet was developing beyond the previously closed scientific community from which it originated into more commercial settings, governmental regu-

---

9 Anna E Shimanek, "Do You Want Milk With Those Cookies?: Complying With The Safe Harbour Principles" (Winter 2001) 26 J Corp L 455 at 4.

10 This is calculated using figures that are supplied by the online "swipe toolkit" an online tool that provides rates charged by data mining services that are not generally made available to the public. See generally Beatriz da Costa, Jamie Schulte & Brooke Singer, "Swipe toolkit", online: Turbulence <http://www.turbulence.org/Works/swipe/main.html>.

11 Shimanek, *supra* note 9 at 4.

12 The technology that led to the development of modern hard disks was recognized in the awarding of the 2007 Nobel Prize in physics. See for example Kevin Bullis, "Hard Drive Advance Wins the Nobel Prize" (10 October 2007) online at <http://www.technologyreview.com/computing/19501/>.

13 Federal Trade Commission, ed, Federal Trade Commission Roundtable Series 1 on: Exploring Privacy (7 December 2009) (Washington: Federal Trade Commission, 2009), online at <http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec2009_Transcript.pdf> at 18 [Privacy Workshop 1].

lators were faced with a dilemma on how best to proceed from a regulatory perspective. In 1997, the White House published a document that would have global implications on Internet policy entitled "A Framework for Global Electronic Commerce." It set out the Clinton administration's view of how Internet regulation ought to proceed.[14] The framework took a hands — off approach, choosing to see how industry preferred to deal with issues as they arose through self-regulation, technological advancement and consumer education.[15] In its general tenor, the framework takes the view that governmental regulation at the interim stage would only serve to interfere with the marketplace and made it clear that the private sphere was to take the lead in self-regulation and developing the standards and policies that could meet consumer expectations.[16] With respect to privacy, the framework took the same approach with the added caveat that if effective privacy protection could not come from the private sector, the administration would re-evaluate this policy.[17] The document is significant because it framed the initial discourse surrounding Internet regulations in the years that followed and had broad global implications as well.

(c) The Canadian Approach: PIPEDA

Canada would follow a different approach in its method of addressing consumer privacy concerns in the private sector. In assessing the impact of the technological changes that were taking place in the late 1990's, the Canadian government decided to take a more active approach to privacy regulation than their American counterparts. Moreover, the government wished to avoid any difficulties that faced entities outside of the European Union (EU) that were subject to that jurisdiction's new privacy directive. Indeed, this Directive forced the United States to negotiate a safe harbor agreement with the EU in order to ensure continued access to the EU marketplace for American companies.[18] To this end, Canada enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[19]

PIPEDA is broad in its application and applies to virtually all commercial activity in Canada.[20] The Act applies to the federally regulated private sector and to provincially based organizations that disclose the information they collect for consideration outside of provincial boundaries.[21] Three years following its proclamation, the Act applied to all organizations in the private sector that "collect, uses or discloses" personal information in the course of commercial activity regardless of

---

14 See generally William Jefferson Clinton & Albert Gore Jr "A Framework for Global Electronic Commerce" (Washington, DC: The White House, 1997), online: <http://clinton4.nara.gov/WH/New/Commerce/read.html>.

15 *Ibid.*

16 *Ibid.*

17 *Ibid.*

18 Shimanek, *supra* note 9 at 458.

19 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

20 Teresa Scassa, "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation" (2000 / 2001) 32 Ottawa L Rev 1 at 4.

21 PIPEDA, *supra* note 19 s 30(1).

lators were faced with a dilemma on how best to proceed from a regulatory perspective. In 1997, the White House published a document that would have global implications on Internet policy entitled "A Framework for Global Electronic Commerce." It set out the Clinton administration's view of how Internet regulation ought to proceed.[14] The framework took a hands — off approach, choosing to see how industry preferred to deal with issues as they arose through self-regulation, technological advancement and consumer education.[15] In its general tenor, the framework takes the view that governmental regulation at the interim stage would only serve to interfere with the marketplace and made it clear that the private sphere was to take the lead in self-regulation and developing the standards and policies that could meet consumer expectations.[16] With respect to privacy, the framework took the same approach with the added caveat that if effective privacy protection could not come from the private sector, the administration would re-evaluate this policy.[17] The document is significant because it framed the initial discourse surrounding Internet regulations in the years that followed and had broad global implications as well.

(c) The Canadian Approach: PIPEDA

Canada would follow a different approach in its method of addressing consumer privacy concerns in the private sector. In assessing the impact of the technological changes that were taking place in the late 1990's, the Canadian government decided to take a more active approach to privacy regulation than their American counterparts. Moreover, the government wished to avoid any difficulties that faced entities outside of the European Union (EU) that were subject to that jurisdiction's new privacy directive. Indeed, this Directive forced the United States to negotiate a safe harbor agreement with the EU in order to ensure continued access to the EU marketplace for American companies.[18] To this end, Canada enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[19]

PIPEDA is broad in its application and applies to virtually all commercial activity in Canada.[20] The Act applies to the federally regulated private sector and to provincially based organizations that disclose the information they collect for consideration outside of provincial boundaries.[21] Three years following its proclamation, the Act applied to all organizations in the private sector that "collect, uses or discloses" personal information in the course of commercial activity regardless of

---

14 See generally William Jefferson Clinton & Albert Gore Jr "A Framework for Global Electronic Commerce" (Washington, DC: The White House, 1997), online: <http://clinton4.nara.gov/WH/New/Commerce/read.html>.

15 *Ibid.*

16 *Ibid.*

17 *Ibid.*

18 Shimanek, *supra* note 9 at 458.

19 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

20 Teresa Scassa, "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation" (2000 / 2001) 32 Ottawa L Rev 1 at 4.

21 PIPEDA, *supra* note 19 s 30(1).

whether or not that entity falls under federal or provincial jurisdiction.[22] An exception exists for those provinces that have enacted legislation that is deemed to be equivalent.[23] This legislation may apply to all commercial activity generally within a province or to particular sectors. Those sectors that are not regulated are then governed by PIPEDA.[24] The Act itself is based upon the model privacy code adopted by the Canadian Standards Association[25] and relies upon the office of the Privacy Commissioner of Canada to enforce its various provisions.[26]

(d) The Federal Trade Commission and Privacy Regulation

Consumer privacy in the United States is protected through the operations of the Federal Trade Commission (FTC). In 1995, the FTC Bureau of Consumer Protection undertook a consumer Privacy Initiative to educate consumers and businesses about the use of personal information on the Internet.[27] A set of hearings was then held which culminated with the release of a staff report entitled the "Public Workshop on Global Privacy and Information Infrastructure." This report concluded that the principles of notice, choice, access and security were recognized as necessary to enable the development of fair information practices online.[28] The report trumpeted the potential for technological solutions, combined with industry self-regulation as a means of addressing online privacy concerns.[29] The primary means by which the FTC would intervene in privacy matters was through the appli-

---

22 Exemptions from the application of PIPEDA include: (i) non-commercial activities, (ii) charities, universities, schools or hospitals, (iii) the professions except where these organizations are engaged in commercial activities, (iv) employee records in the provincially regulated private sector, (v) agents of the Crown in right of the Province, or (vi) municipalities. See Michael Power, "Bill C-6: Federal Legislation in the Age of the Internet" (1999) 26 Man LJ 235 at 238.

23 PIPEDA, *supra* note 19 s 26(2)(b).

24 *Ibid.*

25 Scassa, *supra* note 20 at 6.

26 PIPEDA, *supra* note 19 s. 12.

27 Thomas P Vartanian Robert Ledig & Lynn Bruneau, *21st Century Money, Banking and Commerce* (Washington: Fried, Frank, Harris, Shriver and Jacobson, 1998) at 309.

28 *Ibid.* Briefly, the four principles are:

> 1. Businesses should provide *notice* of what information they collect from consumers and how they use it;
>
> 2. Consumers should be given *choice* about how information collected from them may be used;
>
> 3. Consumers should have *access* to data collected about them; and
>
> 4. Businesses should take reasonable steps to ensure the *security* of the information that they collect from consumers.

See Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Preliminary FTC Staff Report) (Federal Trade Commission: Washington D.C., December 2010) at 7 [FTC Report].

29 Vartanian, *supra* note 27 at 309.

cation of Section 5 of the FTC Act that would allow the commission to take action against deceptive or unfair acts or practices.[30] This is in keeping with the sectoral approach that prevails in the United States where the FTC also is responsible for enforcing numerous sector specific statutes relating to consumer privacy including[31] the *Gramm-Leach-Bliley Act*,[32] the *Children's Online Privacy Protection Act*,[33] the *CAN — SPAM Act*,[34] and the *Telemarketing and Consumer Fraud and Abuse Prevention Act*.[35] The FTC has used its authority under various statutes to bring 29 cases against businesses that failed to protect consumer information since 2001.[36] The FTC has in the last number of years, confined itself to law enforcement, consumer and business education, policymaking and international outreach in order to advance its consumer privacy initiatives.[37]

One of the difficulties with the aforementioned approach is that throughout its history of regulating private sector privacy rights, the United States has chosen to follow a reactive approach, choosing to regulate sectorally rather than broadly. As a result, privacy regulations that are developed in the United States generally tend to react to events rather than seeking to deter potentially harmful behavior.[38] Unfortunately, when dealing with the Internet context, this approach does not stem the tide of incidents that tend to undermine consumer confidence and hinder the acceptance rates of new technologies that leverage the Internet. By having the FTC step in after an incident has taken place, there exists the risk that insufficient steps are taken to provide for a predictable and stable framework that businesses and consumers can rely upon in order to have their expectations met in the marketplace. The empirical results would confirm a wide gap between these expectations and demonstrate a disparity between consumer perceptions and the state of the law as it presently exists (as is illustrated in the next section).

II. NEW CONSUMER ATTITUDES AND PERCEPTIONS

(a) Consumer Perceptions of Online Advertising and Regulations

As consumers have now built up a history with online technologies, studies are emerging that detail how they perceive privacy protection and provide a view to gauge the effectiveness of previous approaches to meet consumer expectations.

---

30 15 USC §45.

31 FTC Report, *supra* note 28 at 4.

32 15 USC §§6801–6809 (2010).

33 15 USC §§6501–6506 (2010).

34 15 USC §§7701–7713 (2010).

35 15 USC §§6101–6108 (2010).

36 *Ibid* at 10.

37 *Ibid* at 12.

38 Information Policy Commission, National Information Infrastructure Task Force. *Options for Promoting Privacy on the National Information Infrastructure* (1997) at 1. Also available online at <http://www.iitf.nist.gov/ipc/privacy.htm>.

One such study emerged in 2009[39] where the authors conducted a telephone study of Americans of various age groups to get a sense of whether they would welcome the efforts of marketers in providing them with targeted advertising of the products that they wanted. The study provides a number of findings that may be useful for present purposes.

One of the areas of particular concern for participants of this study was the information that was targeted towards them for promotional purposes. The study found that older groups of individuals tended to reject tailored advertisements and other forms of behavioral tracking than younger groups of individuals did.[40] This tends to mirror claims by industry that privacy concerns are particularly heightened in groups of older individuals.[41] However, all age groups were shown to have more tolerance for tailoring and behavioral tracking when the activity provided consumers with discounts rather than with advertising and news.[42] Moreover, every age group was demonstrated to have somewhat more tolerance for behavioral tracking when carried out on the website that they are presently visiting as opposed to having it carried out on subsequent websites that they visit or in physical stores.[43]

With respect to consumer choice as it relates to their abilities to control their personal details, the study found that numerous concerns persist despite industry attempts to reassure consumers. The study found that 47% of respondents agreed, and 20% agreed strongly, that consumers have lost control over how their personal information is collected and used.[44] Despite this fact, the authors found that 53% of respondents agreed, and 5% agreed strongly that most businesses handled information they collected in a proper or confidential way.[45] However, curiously enough, the authors found that a substantial majority of respondents mistakenly assumed that laws do not allow businesses to sell personal information.[46]

When looking at the principles or laws that consumers would expect to see industry follow, the survey results do produce some valuable insights. The authors note that 69% of respondents believed that there should be a law that gives individuals the right to know everything that a website knows about them.[47] In addition, 92% of respondents believed that there should be a law that requires websites and advertising companies to delete all stored information about an individual, if requested to do so; with another 62% of respondents believing that advertisers should be required by law to immediately delete information about their Internet activity.[48]

---

39 Joseph Turow et al, "Americans Reject Tailored Advertising and Three Activities That Enable It" (29 September 2009), online: SSRN <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214> [Turow Study].

40 *Ibid* at 19.

41 *Ibid* at 9.

42 *Ibid* at 19.

43 *Ibid.*

44 *Ibid.*

45 *Ibid.*

46 *Ibid* at 20.

47 *Ibid.*

48 *Ibid.*

Moreover, some 70% of respondents stated that companies should be fined more than the $2500 hypothetical maximum fine suggested by the surveyors in the event that a company purchases or uses an individual's information illegally.[49]

Similar results can be found in a recent study that was undertaken for the Canadian Privacy Commissioner's Office by the polling firm Harris Decima in 2011. This study also relied upon telephone interviews across various age groups.[50] Here as was the case in the United States, older individuals were more likely to agree with the statement that businesses take seriously their responsibility to protect consumer personal information (7% for those under age 34 versus 31% for those over the age of 34).[51] However, the authors of the survey concede that rather than believing the converse to be true, the younger group was more likely to indicate that businesses were taking their duty to protect individual privacy "somewhat" seriously instead.[52]

With respect to Canadian attitudes with respect to the uses that businesses put personal information, the study finds considerable apprehension. For example, 67% of respondents stated that they were most concerned about their information being sold to third parties.[53] With respect to receiving unwanted communications from businesses, 57% indicated that they were very concerned. An additional 55% stated that they were concerned about businesses requesting too much personal information about them.[54] It is noteworthy that the authors state that for each of the issues raised in the private sphere context, only one in ten consumers of all age groups stated that they were not concerned about it.[55]

The study also confirms that Canadians, also share the suspicions regarding the loss of privacy voiced by Americans above. Almost sixty percent of respondents agreed that they felt that they had less protection of their personal information in their daily lives than they did ten years ago.[56] Another 65% of respondents rated their knowledge of personal privacy rights as either poor or neutral.[57] When discussing the privacy policies notices that are provided to consumers, the study finds that a small majority agreed with the statement that privacy policies are unclear.[58] Curiously though, the study did find that privacy policies are more often read by younger Canadians than by seniors.[59] As was the case in the United States, Cana-

---

49 *Ibid.*

50 Harris Decima, "2011 Canadians and Privacy Survey Report Presented to the Office of the Privacy Commissioner of Canada" (Ottawa: Harris Decima, 2011), online: Privacy Commissioner of Canada <http://www.priv.gc.ca/information/survey/2011/por_2011_01_e.pdf>.

51 *Ibid* at 14 and 32.

52 *Ibid* at 14.

53 *Ibid.*

54 *Ibid.*

55 *Ibid.*

56 *Ibid* at 19.

57 *Ibid* at 10.

58 *Ibid* at 36.

59 *Ibid* at 37.

dian consumers also wish to see severe sanctions imposed on businesses that violate their privacy commitments to their customers. When asked whether a delinquent organization be legally required to put in place the necessary privacy protections, 97% of all respondents answered affirmatively. Moreover, 95% thought that the offending organization be named publically, while 91% of respondents thought it would be appropriate to fine the organization and 84% thought an offending organization should be taken to court.[60] Similar results can be found in a new survey commissioned by the European Commission to gauge consumer attitudes in the EU.[61]

The conclusions that can be drawn from these studies are important. First, it is quite remarkable that despite over 15 years of experience with the Internet and online commerce, North American consumers still exhibit significant apprehension with respecting the security of their personal details online. In addition, consumers still do not possess an accurate knowledge of common contractual terms and regulations that pertain to informational privacy and behavioral advertising. However, notwithstanding industry efforts of reassurance and new technological and product development, the studies would seem to suggest that consumers have yet to feel totally empowered in their ability to control their personal details and browsing habits. Secondly, despite the fact that the Internet is prominent in everyday life and more and more individuals are becoming familiar with its underlying infrastructure, consumers still remain largely unaware of the uses to which their personal information is being put. Once they become aware of the manner in which personal details are used to generate revenue for private companies, the studies would confirm that there is considerable consumer resentment that follows.[62]

One possible explanation for this confusion may arise from the private contractual terms that typically govern consumer transactions. The initial belief in a hands — off approach outlined above led to the conclusion that market discipline could be borne on companies with an online presence to ensure that contractual terms would fall into line with consumer expectations with the possibility of state intervention should this prove not to be the case. However, what has been witnessed in recent years would suggest that rather than reflecting a bargain among equals, privacy agreements are exhibiting traits that consumer protection advocates would describe as unequal bargaining, where there is an informational asymmetry commonly found when the issue of unconscionability is assessed in consumer sales contracts.[63] Indeed, one recent study had this to say about the current state of privacy policies that predominate online:

> Reading current online privacy policies is challenging and time consuming. It is estimated that if every Internet user read the privacy policies for each

60 *Ibid* at 17.

61 See generally TNS Opinion and Social. *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*. (Brussels: TNS Opinion & Social, 2011), online: European Union <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf>.

62 Turow Study, *supra* note 39 at 20.

63 See generally Jacob S Ziegel & Anthony J Duggan. *Commercial and Consumer Sales Transactions*, 4th ed, (Toronto: Emond Montgomery, 2002) at 101–106.

> site they visited, this lost time would cost about $781billion per year. It is admittedly unrealistic to expect consumers to read and understand the privacy policy of every site they visit. Most policies are written at a level that is suitable for consumers with a college level education and use specific domain technology that consumers are frequently unfamiliar with. Rarely is a policy written such that consumers have a clear understanding of where and when their data is collected, how and by whom it will be used, if it will be shared outside of the entity that collected it, and for how long and in what form it will be stored. Even worse, it is unlikely consumers will even read a single policy given a widespread consumer belief that there are no choices when it comes to privacy: consumers believe they do not have the ability to limit or control companies' use of their information. [footnotes omitted][64]

The question remains however, why hasn't informed consent become more prominent in the ensuing years through consumer education provided by companies seeking to alley consumer fears? One possible explanation, comes from Richard Purcell, the CEO of the Corporate Policy Privacy Group and present Chairman of the Data Privacy and Integrity Advisory Committee for the U.S. Department of Homeland Security, who stated that some of the major reasons for the lack of corporate outreach vis-à-vis consumer education are the result of:

> 1. Monetary Issues that result from the expensive nature of these programs; and
>
> 2. Liability issues associated with having straightforward privacy policies that may leave many commercial actors exposed.[65]

With respect to this latter point, Purcell notes that companies would prefer to have their lawyers draft dense privacy policies to mitigate against this risk rather than engage in consumer education.[66]

III. NEW PARADIGMS AND PROPOSALS FOR REFORM

(a) A New Approach: Privacy by Design

Despite the fact that regulators have waited to see how market dynamics will affect privacy regulation in the private sphere, existing approaches have begun to change so as to reflect a change in philosophy from the original notice and choice paradigm towards an approach that plays a more active role in ensuring that consumer rights are respected. One of the newer approaches that have been adopted by the FTC is one that is pioneered by the Information and Privacy Commissioner of the Province of Ontario, Canada through the concept of "Privacy by Design." This approach emphasizes the fact that all service providers seek to incorporate elements that safeguard consumer privacy at the outset, before product development takes place rather than examining the privacy implications of proposed technologies after

---

64 Patrick Gage Kelley et al, "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach" (2010), online: Carnegie Mellon University Cylab <http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf> at 1.

65 Privacy Workshop 1, *supra* note 13 at 54-55.

66 *Ibid* at 55.

they have been developed.[67]

The Privacy by Design approach encourages companies to incorporate substantive privacy protections into their practices such as data security, reasonable collection limits, develop sound retention policies and ensure data accuracy.[68] In its legal manifestation, the approach centers on the development of legal rules and practices that recognize individual privacy rights throughout the life cycle of a product, program or service.[69] Moreover, it is stressed that under this framework, regulations should encourage the development of privacy policies that are consistent with the applicable mechanisms required or provided to give effect to individual choice.[70] In a recent report, the FTC emphasizes that companies should consider privacy issues systemically at all stages of the design and development of products and services.[71] By doing so, the FTC hopes to empower consumers by safeguarding their privacy without forcing them to read long notices to determine whether basic privacy protections are offered.[72] Privacy by Design represents a departure from previous models by emphasizing to policy developers that the changing nature of the Internet and the ongoing advancement of technology necessitates a change in approach that begins with the premise that consumer information ought to be protected and that technological developments should be built around this principle rather than being a mere afterthought.[73]

Although this is a relatively straightforward proposition, it has the potential to significantly reduce transactions costs if the privacy ramifications that flow from technological developments could be identified and corrected from the design stage before the product is released to the public rather than the present reactionary approach. The Privacy by Design approach has found a receptive audience throughout the world as policymakers debate how best to regulate the Internet following recent developments and the ever changing nature of Internet technologies. In a recent report, the FTC expressed its support for the Privacy by Design approach that has been championed by the Ontario Information and Privacy Commissioner Ann Cavoukian.[74]

As part of its strategy to implement a Privacy by Design Framework, the FTC has identified four main themes that it identifies as building blocks that can be applied to all commercial entities that collect or use consumer information.[75] This

---

67 Ann Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision — Makers and Policy — Makers* (Toronto: Privacy Commissioner of Ontario, 2011), online: Privacy by Designivacybydesign.ca/content /uploads/2011/08/pbd-law-policy.pdf> at 10.

68 FTC Report, *supra* note 28 at 41.

69 Cavoukian, *supra* note 67 at Appendix B.

70 *Ibid.*

71 FTC Report, *supra* note 28 at 44.

72 *Ibid.*

73 For a further elaboration of what principles ought to govern actor behavior in the Privacy by Design framework, see Cavoukian, *supra* note 67 at Appendix A.

74 FTC Report *supra* note 28 at 41.

75 It is these four themes that will collectively be referred to as the "Privacy by Design" approach hereinafter.

includes:

1. *Scope*;
    - The proposed framework applies to all commercial entities that collect consumer data that can be reasonably linked to a specific consumer, computer, or other device
2. *Privacy by Design*;
    - Whereby companies are encouraged to incorporate substantive protections into their practices and at every stage of the development of their products and services
3. *Simplified Choice*;
    - For practices requiring choice, companies should offer the choice at a time and context in which the consumer is making a decision about his or her data.
4. *Greater Transparency*.[76]
    - Whereby companies should increase the transparency of their data practices. This can take place through notices that are provided to consumers that should be clearer, shorter and more standardized in order to enable better consumer comprehension and comparison of privacy practices

The Canadian Privacy Commissioner has also proposed similar suggestions.[77]

Of particular interest for present purposes here is the elaboration offered by the FTC regarding instances where consumers may be called upon to consent to the use of their data. Not surprising, the FTC recommends that consumers be given the opportunity to make *meaningful* and *informed* choices with respect to what may be done with their information at a time and context in which the consumer is making a decision about their data.[78] Moreover, the FTC has been endorsing an approach that would provide consumers with the ability to opt out of behavioral tracking efforts of industry by providing consumers with the option to click on an icon that would appear on targeted advertisements giving consumers the option to choose a "do not track" option.[79] This is also an option that could be built into the web browsing software that consumers use to access the Internet.[80]

(b) Consumers Should Have a Proprietary Right in their Information

One of the fundamental principles that ought to be enshrined in any new regulatory developments governing consumer privacy is that consumer information ought to belong to the consumer. Indeed, this sentiment was echoed by Nicole Ozer

---

76 FTC Report, *supra* note 28 at 41.

77 Privacy Commissioner of Canada. *Privacy Trust and Innovation — Building Canada's Digital Advantage* (Ottawa: Privacy Commissioner of Canada, 2010), online: Privacy Commissioner <http://www.priv.gc.ca/information/pub/sub_de_201007_e.pdf> at 11-12.

78 FTC Report, *supra* note 28 at 57-58.

79 *Ibid* at 63-64.

80 *Ibid* at 64.

from the ALCU of Northern California at one of the three FTC privacy roundtables held over the course of the last two years:

> I found this quote from the Senate Judiciary record that said very clearly: "For the person or business whose records are involved, the privacy or proprietary interest should not change."
>
> I think that's a really important issue because the core concept of making sure that just because my information has gone to one company who then has shared it or has been doing services or storing it with many other companies doesn't mean that initial control shouldn't still reside with the initial consumer.[81]

Indeed, this should be the starting point of any efforts to instill a Privacy by Design approach to technological developments. Taking the argument further, it may warrant enacting legal provisions that would deem personal details (including the individual's image) to be the property of the individual at all times and that all that they may grant a third party is a license to use this information — one that can be revoked at any time on the happening of certain events. Moreover, in cases where the original entity that obtained the consent ceases to exist (or is declared insolvent), the license would be deemed to revert to the owner. With respect to this latter point, consider the effect that insolvency has respecting the promises made by companies to their customers' privacy.

(c) Toysmart Case

A number of high profile incidents have shown that in companies have preferred to monetize consumer data as an asset to maintain their business as a going concern or make their assets more lucrative for an acquirer. Consider for example the rise and subsequent fall of a website called Toysmart.com that was launched in early 1999 and offered consumers an opportunity to purchase discount toys online.[82] The website attempted to build consumer confidence by becoming a licensee of TRUSTe which is a prominent online organization that reviews and certifies that its member's online privacy policies conform to their standards. TRUSTe is in essence a branding institution through which consumer recognition is meant to serve as an economic incentive for companies to conform to their regulations.[83]

On its website, Toysmart assured its customers that none of the information that its customers voluntarily disclosed would be shared with a third party. Toysmart was a losing business proposition and involuntarily declared bankruptcy in June, 2000. Prior to the filing, Toysmart contracted the services of a management consulting firm and listed among its assets various "Intangibles, i.e., URL name, databases, customer lists, marketing plans, website content, software intellectual property."[84] This statement appeared in an advertisement in the *Wall Street Journal*

---

81 Federal Trade Commission, ed, Federal Trade Commission Roundtable Series 2 on: Exploring Privacy (28 January 2010) (Washington: Federal Trade Commission, 2010), online: <http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf> at 193.

82 Winn *supra* note 3 at 9.

83 See for example the Truste website: <www.truste.com>.

84 Winn, *supra* note 3 at 10.

and provoked a public outcry. The FTC in turn, filed a complaint in the bankruptcy case seeking a permanent injunction against the sale of Toysmart customer lists and a declaration that the sale constituted a contravention of the FTC Act in light of Toysmart's own privacy representations.[85] Toysmart eventually settled with the FTC whereby it would be allowed to sell its customer lists to a buyer "in a related market."[86]

(d) Borders Books and Music Bankruptcy

In 2011 the well-known bookseller and media retailer Borders Group was forced into bankruptcy.[87] The chain could find no bidders for the business as a going concern and was then forced to liquidate its assets.[88] In the course of liquidating its assets, the court received a bid from Borders' rival, Barnes and Noble, for the intellectual property assets of the company.[89] Included as part of the sale were the rights to the Borders trade name, and the company's website and social media presences.[90] Of particular interest to Barnes and Noble, was the customer lists of Borders, particularly information concerning members of the Borders loyalty program, *Borders Rewards*, whose members Barnes and Noble had hoped would be transitioned into the Barnes and Noble ecosystem.[91]

One potential barrier to the transaction came in the form of the privacy policy that governed the *Borders Rewards* program for members that had joined prior to 2008. In a court filing, the Consumer Privacy Ombudsman appointed by the Court to oversee the sale of the intellectual property of Borders had argued that pursuant to the pre — 2008 privacy policy that limited the transfer of *Borders Rewards* data to third parties, Barnes and Noble be required to contact all members of *Borders Rewards* that had signed up for the program prior to 2008 to obtain their consent to the transfer.[92] Barnes and Noble responded by stating that the consent requirement was "completely unrealistic" since the requirement could cause the assets to lose

---

85 *Ibid.*

86 *Ibid.* This is discussed further below.

87 Tiffany Kary & Linda Sandler, "Borders Files Bankruptcy, Is Closing up to 275 Stores", online: Bloomberg Businessweek <http://www.businessweek.com/news/2011-02-16/borders-files-bankruptcy-is-closing-up-to-275-stores.html>.

88 Tiffany Kary "Borders Liquidators Race Clock, Squeeze Cash from 200 Stores" (29 March 2011) online: Bloomberg Businessweek <http://www.businessweek.com/news/2011-03-29/borders-liquidators-race-clock-squeeze-cash-from-200-stores.html>.

89 Jeff Roberts, "B&N, Others Buy Borders Intellectual Property For $15.8 Million" (16 September 2011) online: Paid Content:The Economics of Content<http://paidcontent.org/article/419-bn-others-buy-borders-intellectual-propery-for-15.8-million>.

90 *Ibid.*

91 Jeff Roberts, "Privacy Policy May Sink B&N's Purchase of Borders Name" (22 September 2011) online: Paid Content: The Economics of Content <http://paidcontent.org/article/419-privacy-policy-may-sink-bns-purchase-of-borders-name>.

92 *Ibid.*

value and thereby put the transaction as a whole "at risk."[93] Barnes and Noble proposed using their own privacy policies that it argued were equivalent or offered greater protection than the existing Borders policy.[94]

The FTC intervened by writing to the Privacy Ombudsman and expressed its concerns regarding whether or not Borders' actions would constitute an unfair or deceptive trade practice.[95] The FTC noted the discrepancy between the original Borders privacy policy announced in 2006 and the subsequent substantive amendment in 2008. In particular, the 2006 policy stated:

> Borders, Inc., Walden Book Company, Inc., and their related companies believe that your personal information — including your purchase history, phone number(s), and credit card data — belongs to you. We collect this type of information to serve you better when you provide it to us, but we do not rent or sell your information to third parties. From time to time, we may ask if you are interested in receiving information from third parties whose services or information we think would be of value to you. In those instances, we will only disclose your email address or other personal information to third parties *if you expressly consent to such disclosure*. (Emphasis in original).[96]

In 2008, the policy was amended through the addition of an additional clause that was found at the end of the policy:

> Circumstances may arise where for strategic or other business reasons, Borders decides to sell, buy, merge or otherwise reorganize its own or other businesses. Such a transaction may involve the disclosure of personal or other information to prospective or actual purchasers, or receiving it from sellers. It is Borders' practice to seek appropriate protection for information in these types of transactions. In the event that Borders or all of its assets are acquired in such a transaction, customer information would be one of the transferred assets.[97]

It is relevant to note that the amendment came shortly after the chain was first experiencing financial difficulties and management was actively seeking a sale of the company.[98] The FTC took the position that while this change may have been necessitated by the need to continue the business as a going concern, it was not

---

93 Nick Brown, "Privacy Throws Snag in B&N — Borders IP Deal", (21 September 2011) online: Thomson Reuters <http://newsandinsight.thomsonreuters.com/bankruptcy/news/2011/09_-_September/Privacy_terms_throw_snag_in_B_N-Borders_IP_deal>.

94 Michael Cooney, "Privacy Stink Erupts over Borders Bankruptcy Deal", online: Network World Community <http://www.networkworld.com/community/blog/privacy-stink-erupts-over-borders-bankruptcy>.

95 Federal Trade Commission, "Letter to Michael Baxter and Yaron Dori", online: Federal Trade Commission <http://www.ftc.gov/opa/2011/09/borders.shtm> [FTC Letter to Baxter].

96 *Ibid.*

97 *Ibid.*

98 Scott Moritz, "Borders Hoists For Sale Sign" (20 March 2008) online: CNN Money <http://money.cnn.com/2008/03/20/news/companies/Moritz_borders.fortune/?postversion=2008032011>.

meant to provide for a piecemeal sale of the company's assets in a bankruptcy liquidation.[99]

The facts of this case strongly resemble the Toysmart case above. Consequently, the FTC sought to use the same framework that it had developed in the Toysmart case, where the sale of customer information was allowed in limited circumstances.[100] Ultimately, Barnes and Noble agreed to give pre — May 2008 *Borders Rewards* members the right to opt in to the Barnes and Noble customer lists.[101] However, the proposed settlement did not meet the privacy ombudsman's satisfaction. It unsuccessfully attempted to obtain additional protections for consumers since the company argued that the ombudsman had no approval rights over the specific wording of the privacy email that was sent to Borders customers.[102]

These two incidents demonstrate some of the dangers that are associated with allowing companies to deal with personal information following an insolvency. As the Borders incident demonstrates, consumers may have agreed to provide a company with their personal details only to find out that they have become a "customer" (along with their history) of a company that they may never have done business with. Allowing a company to monetize this information may allow a company to attempt to leverage its assets and continue as a going concern. However, what is troubling about the Toysmart and Borders examples is that the interests of consumers were not considered by each company as they sought to satisfy the claims of their creditors after they became insolvent. It is unfair to ask consumers to tolerate invasions of their privacy. Instead, creditors rather than consumers are in the best position to absorb the loss. Consumers should be given the option to decide whether they are prepared to become the customer of a company and what information they will give it access to rather than having that information transferred as part of a transaction that flagrantly ignores the representations under which the consent was originally given.

(e) Sears Holdings Tracking Software

As described above, one of the difficulties with present privacy practices is that there exists a tremendous temptation for companies to monetize the use of

---

99 FTC Letter to Baxter, *supra* note 95.

100 In this case, the FTC had argued that its concerns could be allayed if the following conditions were met:

- Borders agrees not to sell the customer information as a standalone asset;
- The buyer is engaged in substantially the same lines of business as Borders;
- The buyer expressly agrees to be bound by and adhere to the terms of Borders' privacy policy; and

The buyer agrees to obtain affirmative consent from consumers for any material changes to the policy that affect information collected under the Borders' policy. See FTC Letter to Baxter, *supra* note 95.

101 Katy Stech, "Barnes and Noble Email to Borders Customers Rattles Privacy Watch–dog" (4 October 2011) online: Wall Street Journal <http://blogs.wsj.com/bankruptcy/2011/10/04/barnes-noble-email-to-border-customers-rattles-privacy-watchdog>.

102 *Ibid.*

data. Indeed, this temptation may prove to be too great and risk violating the trust of their customers. For example, in 2009, the FTC brought forward a complaint against Sears Holdings Management Corporation,[103] the corporation that owns the K-Mart and Sears retail chains. The dispute centered on an initiative that Sears developed called "My SHC Community" where customers of the two chains were offered the opportunity to interact with Sears Holdings to alert the company of the products and services its customers desired.[104] In exchange for ongoing special offers, draws, and $10 after the first month of active membership, customers were asked to download software that was designed to track their online activities.[105] The scope of the information that was collected was quite intrusive in scope; the software recorded and transmitted information pertaining to the contents of consumer shopping carts, online bank statements, drug prescription records, video rental records and library borrowing histories.[106]

Enrollment in the program occurred through a multi-registration process that disclosed various representations about the manner in which information was to be collected and used. First, customers were required to submit an email address to Sears. The email submission resulted in a message sent to the user's account in which more information was provided with respect to the program and a link displayed where customers could proceed to the actual registration.[107] This email message stated that the software would confidentially track a users' online browsing, but that the user would decide when and how to journal this information with the option of uninstalling the software at any time.[108] After proceeding to the embedded link, the user was then directed to the download site where the privacy policy that would govern this arrangement was located[109] (it is interesting to note that this was a policy that was separate from the main Sears and K-Mart privacy policies).[110] It was only in the privacy policy that was posted to consumers on this download page, that the company disclosed the true nature of the scope of the information that was to be collected.[111] The section read as follows:

> Once you install our application, it monitors all of the Internet behavior that occurs on the computer on which you install the application, including both your normal web browsing and the activity that you undertake during secure sessions, such as filling a shopping basket, completing an application form or checking your online accounts, which may include personal financial or

---

103 *In re Sears Holdings Management Corporation* (31 August 2009), C-4264, online: FTC <http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf> (Sears Consent Order).

104 See *In re Sears Holdings Management Corporation* (31 August 2009), C-4264, online: FTC <http://www.ftc.gov/os/caselist/0823099/090604searscomplaintaf.pdf> (Sears Evidence).

105 *Ibid.*

106 FTC Report, *supra* note 28 at 13.

107 Sears Evidence, *supra* note 104 Exhibit A.

108 *Ibid* Exhibit B.

109 *Ibid* Exhibit D.

110 *Ibid* Exhibit E.

111 *Ibid.*

> health information. We may use the information that we monitor, such as name and address, for the purpose of better understanding your household demographics; however we make commercially viable efforts to automatically filter confidential personally identifiable information such as UserID, password, credit card numbers, and account numbers. Inadvertently, we may collect such information about our panelists; and when this happens, we make commercially viable efforts to purge our database of such information.
>
> The software application also tracks the pace and style with which you enter information online (for example, whether you click on links, type in webpage names, or use shortcut keys), the usage of cookies, and statistics about your use of online applications (for example, it may observe that during a given period of use of a computer, the computer downloaded X number of bytes of data using a particular Internet enabled gaming application).[112]

This policy might well appear to be a much more intrusive level of monitoring then a reasonable consumer might assume to be the case from the company's initial representations that consumers would have control over when and how any information would be collected. Even where confidential information was to be captured by the software, the company limited its efforts to purging information so long as the efforts were "commercially viable" — which would seem to suggest that economic considerations rather than a desire to maintain individual privacy were to be of overriding importance for the company. Moreover, the privacy agreement also contained the caveat that the company would be allowed to retain and use any information that was collected before a consumer's "resignation" from the program.[113]

The matter was subsequently resolved when Sears signed a consent order with the FTC. Under its terms, Sears was obliged to prominently display the intended uses of the program on a separate screen, prior to the display of the end user agreement and list the types of data that the program was intended to monitor.[114] In addition, Sears was ordered to obtain the express consent of any future participants by requiring them to actively opt — in to participating in the program without a default pre-selected opt — in option that signified consent in the original program.[115] Moreover, Sears was ordered to provide existing participants with the details of the data collected by the program (displayed on the program's website) and provide consumers with support in uninstalling the program if they so wished.[116] Finally, Sears was required to cease collecting and destroy any data collected prior to the filing of the consent order.[117]

The Toysmart, Borders and Sears examples demonstrate that once control of personal information shifts away from a consumer, there really is no limit to what

---

112 *Ibid* Exhibit D.

113 See Sears Consent Order, *supra* note 3 at 4.

114 *Ibid* at 3-4.

115 *Ibid* at 4.

116 *Ibid.*

117 *Ibid* at 5.

legally can be done with that information. As seen in the Borders case, a company that is faced with a precarious financial outlook may ignore any negative repercussions to its goodwill and go back on its word to its consumers. The Sears case demonstrates that commercial pressures and considerations alone will, in some cases, act as a disincentive to meet consumer expectations. By deeming property in the hands of an entity to be the property of the individual concerned, it is possible to hinder the unauthorized trade and use of this information since any transfer will be negated by the operation of the *nemo dat quod non habet* rule.[118]

The proposition that information about an individual remains their property at all times may seem quite radical, particularly when considered against developments in privacy law over the past century. After all, it could be claimed that such a proposition will be too onerous and impose very burdensome transactions costs that will all but eliminate any returns to scale that can be brought through advances in data mining. However, while some costs may increase, the greater good will be advanced, transactions costs that exist due to falling consumer confidence will be reduced, and disproportionalities in bargaining power amongst market actors redressed if steps are taken to correct some of the market failures that presently exist. One of the benefits that this type of approach gives us is that it helps to *de-monetize* the trade in personal details, thereby limiting some of the financial incentives that led to some of the unfortunate incidents described above.

While the proposition may seem far-reaching when viewed against the backdrop of the conventional 1990's / 2000's privacy law doctrines, it is not without precedent when considered against other areas of the law that seek to preserve the confidentiality of customer information. For example, most common law jurisdictions make the disclosure made by clients to their lawyers' privileged information that cannot be disclosed to any third party for any reason. Similar provisions are in place for other types of relationships as well.[119] Of course, the well-known reason for this provision is that societies value certain relationships and we wish to foster an atmosphere where individuals can trust that their information will not be compromised. This is not intended to suggest that the relationship between a customer and merchant ought to be accorded the same deference as a lawyer — client relationship. Rather, the nature of the concept of confidentiality in a professional context demonstrates that in some instances the law will impose certain common law obligations on private parties to take reasonable care with respect to protecting the information that is given to them in the reasonable expectation that this party is motivated primarily by a legal duty of confidentiality towards the disclosing party. Indeed, this would closely resemble the expectations that were raised in the earlier empirical studies that showed that customers expect that their information will be kept confidential when companies promise this in their representations.

When considered more broadly, the legal rationale behind providing a legal duty of confidentiality in certain types of relationships may yield some insights

---

118 The fundamental term in property law that states "one cannot give what one does not have." See generally Clayton P Gillette & Steven D Walt. *Sales Law: Domestic and International*, 2d ed, (New York: Foundation Press, 2009) at 447–453.

119 Consider for instance, doctor — patient, trade secret, confidentiality of journalistic sources and religious communications confidentialities.

when applied to consumer behavioural data. Neil Richards and Daniel Solove have analyzed some of the pre — Warren and Brandeis jurisprudence in the United States with respect to the law of confidentiality. They have found that historically speaking, the law of confidentiality has a long history dating as far back as 1577.[120] They characterized the legal obligations that arise from certain categories of relationships as being a:

> . . . forerunner of the modern body of law of fiduciaries. The law of confidential relations protected a variety of special relationships in which one party entrusted her interests to another. Because the party placing her trust and confidence in the other was extremely vulnerable to harm if the other party abused this trust, the law stepped in to protect this reliance . . . duties of nondisclosure attached to confidential relationships prohibited a person from divulging confidential information to any unauthorized person on pain of liability.[121]

As can be seen, this paradigm can be helpful in establishing a legal framework that protects individuals that disclose sensitive information and helps foster certain relationships. By placing limits on what can be done with information obtained in confidence, the law helps to encourage the candor of the disclosing party that is a necessary precondition to allowing such relationships to develop. Without a free disclosure of this information and legal sanctions for unauthorized disclosure, the functioning of these relationships is hindered since confidence in these relationships would be undermined if vulnerable parties were to be compromised. Consequently, one way of facilitating the exchange of information and allowing society to benefit from advances in technology is to provide consumers with legal assurances that guarantee their privacy choices are respected.

(f) Disclosure and Confidentiality in Commercial Law

While the duty of confidentiality remains a prominent feature of fiduciary type relationships, it is not unheard of in the commercial context. Commercial law is another area where we find similar duties as those enumerated above, respecting the confidentiality that arises as a result of business relationships. Canada and many American States have adopted the English common law rule that banks owe a duty of confidentiality to customers to protect the latters' financial records from unauthorized disclosure of information pertaining to their finances, transaction and financial condition without the customer's actual or implied consent.[122] In general Courts have held that banks implicitly warrant to maintain customer account information in the strictest confidence with certain exceptions.[123] As part of any type of

---

120 Neil M Richards and Daniel J Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Geo LJ 123 at 134.

121 *Ibid* at 135.

122 Vartanian, *supra* note 27 at 291 citing *Tournier v National Provincial and Union Bank of England* (1924), 1 KB 461. See also *Peterson v Idaho National Bank*, 367 P 2d 284 (Idaho 1964) which held that an implied duty of confidentiality exists between a bank and its depositor.

123 *Ibid* at 298. Exceptions have been created in the cases of *Peterson*, *supra* note 122 (where it was held that customer authorization of disclosure and disclosures required

commercial relationship that attempts to consider how to balance privacy rights as determined by a Privacy by Design approach, it would not be difficult to imagine that a framework may emerge in a similar fashion to that described above. Privacy by Design necessitates a re-conception of how business views personal information to remove the monetary temptations that flow from it. Instead, the focus ought to be on helping build confidence in the new emerging technologies in a manner that accord with consumer expectations. By protecting consumer information in this manner, regulation can play a valuable role in advancing the types of technological developments that are more in keeping with what consumers desire, by reducing consumer trepidation and ensuring that vulnerable parties are protected. In this sense, a corresponding advance in confidentiality can help create the conditions that facilitate the growth of certain business relationships much the same way that the law of confidentiality has in the past.

The duty not to disclose is not the only concept from commercial law that may assist regulators seeking to impose a Privacy by Design regime. As seen above, many of the previous approaches to providing meaningful choice to consumers were centered upon creating opportunities to give consumers access to information to make an informed choice. However, as the study by Turrow et al. demonstrates, much of the information that consumers need to access in order to make informed decisions is inaccessible. Moreover, many of the contractual terms that govern privacy relationships are buried in the details of complex legal agreements that are not brought to the immediate attention of consumers.

(g) Nutrition Label Approach

The concept of providing more meaningful and accessible disclosures has found expression in some recent literature. In this vein, a study by Patrick Gage Kelley et al. attempts to provide for a new framework that would clarify and standardize the information that is presented to consumers using a familiar concept — the nutrition label that is commonly found on food products.[124] The study used the nutrition label concept as a summary of the full text commonly found in online privacy policies and tested the outcomes on a sample of 764 individuals in an online study.[125] The study ultimately found that under this format, the accuracy, comparison, and speed results eclipsed the results of the text formats that are presently in use.[126]

The results of the Kelley study confirm what the FTC had been advocating — a more simplified method of allowing consumers to discover contractual terms and

---

by law) and *Barnett Bank of West Florida v Hooper*, 498 So 2d 923 p. 925 (Florida 1986) (where it was held that exceptions to the general rule include disclosures under compulsion of law, pursuant to the public interest, pursuant to a bank's interest, and where expressly or impliedly authorized by the customer); *Graney Development Corporation v Tasken*, 400 NYS 2d 717 (Sup Ct 1978); aff'd 411 NYS 2d 756 (App Div 1978) (holding that the confidentiality duty did not extend to information received by bank from a party to a loan agreement).

124 See generally Kelley et al, *supra* note 64.

125 *Ibid* at 3.

126 *Ibid* at 9.

compare them across different actors in the marketplace. Indeed, this model is a useful method of presenting information to consumers in a manner that allows them to make decision rather quickly while reducing transactions costs and thereby increasing market efficiency. However, while these steps are encouraging, additional steps need to be taken to correct market failures that have undermined consumer confidence in industry efforts to safeguard their privacy.

Moreover, these issues are not new in other areas of the law that have understood the need for governmental regulation in the manner in which information is presented to consumers. Take for instance, new financial regulations pursuant to the Credit Card Accountability Responsibility and *Disclosure Act of 2009*[127] that mandates that disclosures made to consumers in the form of credit card statements must follow a particular format. For example, the new CARD Act requires that information relating to minimum monthly payments, the amount of time that making the minimum payment would take to discharge the total amount owing, the interest rate charged and a toll free number that gives borrowers access to a credit counseling service all be provided in mandatory disclosures included with each credit card statement.[128] The Act also mandates that such disclosures be displayed prominently in a prescribed table format.[129]

Indeed, one of the reason why consumer advocates have argued in favor of mandated disclosures with respect to credit and debit cards has been the result of years of experience with behavior that has undermined consumer confidence in the field of payment products.[130] Credit and Debit card regulation relies heavily on providing consumers with disclosures in order to assist them in minimizing their transactions costs so that they may make informed decisions in the marketplace. Disclosure regimes exist for similar reasons in securities law.[131] As seen through initiatives such as the CARD Act above, transactions costs can be significantly reduced if the information is presented in a standardized format that makes it easy for consumers to have access to the variables that play a crucial role in allowing them to make decisions regarding interest rates, amortization rates etc. Previously, this information along with numerous other onerous terms were found buried within complex contracts written in dense legal jargon.[132] Indeed, one would expect to find that when transactions costs associated with ascertaining and interpreting information are reduced through a predictable and familiar means then the utility of such information brings numerous dividends to increasing consumer awareness. This expectation was confirmed when information was presented in the familiar format of the nutrition label in the Kelley study that showed that a table-based for-

---

127 *Credit Card Accountability, Responsibility and Disclosure Act* (CARD Act) of 2009, Pub L No 111-24, 123 Stat 1734 (to be codified in scattered sections of 15 USC) [CARD Act].

128 *Ibid* at §201(D).

129 *Ibid.*

130 See generally Muharem Kianieff, "Looking for Cover: A Public Choice Critique of the Canadian Debit Card Code" (2006) 37 (1) Ottawa L Rev 101 at 104–107.

131 See Generally Cynthia A Williams, "The Securities and Exchange Commission and Corporate Social Transparency" (1999) 112 (6) Harv L Rev 1197.

132 Joseph Nocera, *A Piece of the Action* (New York: Simon and Schuster, 1994) at 57–62.

mat provided customers with the ability to scan it like a chart and visually look for answers instead of having to read a complex document.[133] More research needs to be done in this area; however the results are consistent with efforts in the payment products sphere to simplify the acquisition and processing of data by consumers.

The preceding would appear to suggest that efforts to situate this information in a familiar format and context would have the greatest probability of success. As such, initiatives that pursue the approach of minimizing transactions costs by presenting information to consumers in a familiar format will best advance the goals outlined by the FTC and assist in the furtherance of a Privacy by Design agenda. The online advertising industry has responded in a similar vein in a bid to ward off potentially onerous legislation.[134] The industry has proposed a privacy icon that would be displayed alongside any advertisements that appear inside a consumer's web browser that they could click on in order to obtain additional information. After clicking on the link, the consumer would be directed to a website that would inform them of how advertisers use web surfing histories and demographic profile to send them certain advertisements.[135] While this is a step in the right direction, it still fails to address many of the shortcomings of the existing approach:

1. how to ensure that the wishes of consumers are respected;
2. that consumers ought to have a say in how their information is used;
3. and does not make fully transparent the uses to which other transactional data may be used in a similar fashion (for example flash cookies that can't be as easily deleted as conventional ones).

Further, regulatory proposals need to take account of information that a consumer will consent to be used by companies in their data analysis. Rather than making the choice one of "take it or leave it," there needs to be some type of middle ground so that when a consumer does decide to grant an entity a license to use their information, they may attach various limitations on the use to which the data may be put. Simply giving consumers a right to unfettered participation with knowledge of what uses their information will be put to is not a meaningful choice for consumers. The usage information needs to allow consumers to make choices; the more choices they have, the greater the chance that they will chose to participate in whatever initiative is proposed to them. This would allow a useful third option to empower consumers that will serve as a middle ground between no participation and unchecked data usage.

(h) Standardization in the Form of Pre-Defined Ratings

It would not be difficult to imagine a change in the status quo that takes into account some of the insights that have been gained in the commercial law context. Here information must be presented in an efficient and easy to read manner to consumers before they enter into certain commercial relationships so that they can

---

133 Kelley et al, *supra* note 64 at 9.

134 Stephanie Clifford, "A Little "i" to Teach About Online Privacy." *The New York Times* (26 January 2010) online: New York Times <http://www.nytimes.com /2010/01/27/business/media/27adco.html>.

135 *Ibid.*

make an informed decision whether to do business with an entity or not. Standardization is used in the nutrition label approach outlined above, but there are also other ways in which information is presented in a standardized fashion. Take for instance, the ratings that individuals rely on for judging the content of motion pictures or televisions programs. These are well-established standards that give individuals an idea of whether the content of this media is inappropriate for certain audiences. Given that these standards are widely publicized, individuals now have some familiarity with the type of content that one would be subject to in a "G" rated movie in contrast to an "R" rated movie.

By the same token, it would not be difficult to envision a legislative scheme being developed to govern licenses granted by consumers to businesses and other organizations to use their data. For instance, might it be possible to present information to consumers in such a manner that consumers could then choose what level of license that they choose to grant an entity seeking permission to gather and use information generated from that particular consumer? Consumers could be presented with a pop up box either in print form or online where they would be provided with disclosure of what the entity seeking their consent seeks to do with their information following pre-defined formats similar to the credit card disclosures discussed above.[136] Consumers could then decide whether to grant the entity consent to use their information, and if so, what level of consent they are prepared to grant to the entity based upon a predefined standard — say "P1" meaning restricted for the immediate purpose requested and then destroyed when no longer required. The stages could vary up to 4 levels with the box reminding the consumer what each level of consent entails. The various levels of consent would also govern the ability of the entity seeking consent to subsequently transfer the consumers' personal information. Moreover, regulations could mandate that any subsequent holders of a consumers' information above the most restrictive setting be bound by the choice made by the consumer or risk revocation of the proprietary license in the information. As part of the existing North American privacy regimes, a governmental authority would be able to enforce compliance with the commitments made by companies to consumers through existing enforcement mechanisms that rely on a complaints driven process thereby relieving consumers from having to take companies that violate these provisions to court.

In order for such a system to remain effective, one of the key objectives to be achieved here must be that consent be made on an opt-in basis. Privacy regulators have been faced with the question of how best to deal the determination of whether consumer consent is informed based on whether they are asked to opt-in or opt-out of a particular privacy policy.[137] Not surprisingly the issue arises in the consumer protection realm as well. Canadians in particular are well familiar with the issue following efforts by the cable television industry in the mid 1990's to impose a new

---

136 A similar concept also exists in the intellectual property realm and its use of creative commons licenses whereby authors are free to specify the types of consent that they are prepared to grant individuals seeking to use their works. This is an alternative to the traditional "all rights reserved" regime. See generally <http://creative–commons.org/about>.

137 FTC Report, *supra* note 28 at 60.

menu of television stations on cable television subscribers on an opt-out basis. Subscribers were required to take action in order to inform their providers that they did not wish to receive the new stations that were automatically added onto their account.[138] The incident was followed by numerous changes to consumer protection provisions to outlaw the practice after a considerable public outrage. While the results may not have satisfied everyone, the practice of requiring consumers to opt-out of services can be viewed as unjust and contrary to the notion of consumer autonomy.[139] By requiring an opt-in by consumers as part of any regulatory regime, we can deny an entity's attempts to rely on a default setting for privacy that may not be brought to the attention of the consumer.

If consumers were presented with a request for permission to access personal information, how would this request be made, taking into account the needs of the entity making the request? If the terms of the request require consumers to opt-in, then an entity would be forced to disclose a level of disclosure that it would require as a minimum to offer the service to the customer. For example, if I access a website, am asked what level of permission I wish to grant, and I offered the lowest setting P1, the entity could then specify that it would require a minimum level of consent at P3 or risk not offering the service to the consumer. The consumer would then be put on notice of what type of uses of their personal information the entity proposes and can know prior to agreeing to the proposed terms exactly what is entailed by acceptance. In this sense, the forced standardization can foster more disclosure between consumers and entities than what presently exists. Presumably, market discipline can be brought to bear on those entities that are seeking an abnormally high privacy rating through negative publicity that is generated in the media and the market at large.

The question remains however, how this proposed regime may remain effective if industry participants collude and uniformly demand the most wide-ranging level of consent available? In all likelihood this will occur with the most established entities that have hitherto effectively monetized the trade in consumer information. However, as new upstart companies and services begin to develop and leverage new technological developments, there may exist incentives to offer more inducements to consumers to begin adopting these new technologies as replacements for legacy channels and this could take the form of offering privacy terms that are more appealing to consumers. Indeed, a number of years ago, few people could have imagined that most individuals shopping for books and music would be doing so from the comfort of their own home. As digital downloads of music became more widespread, online retailers such as iTunes began offering DRM free downloads in response to consumer concerns despite industry opposition.[140] The end result has been nothing short of a radical restructuring of the book and music

---

138 Ziegel and Duggan, *supra* note 63 at 93.

139 See generally Peter Bowal, "Reluctance to Regulate: The Case of Negative Option Marketing" (1999) 36:2 Am Bus LJ 377.

140 Mary Madden, "The State of Music Online: Ten Years After Napster" (June 2009), online: Pew Internet and American Life Project <http://www.pewinternet.org/~/media/Files/Reports/2009/The-State-of-Music-Online-Ten-Years-After-Napster.pdf> at 14-15.

distribution businesses. Consumers have benefited from lower prices and increased flexibility, such as determining how and where they access their music libraries.[141]

It is new nimble entrants to the marketplace (as iTunes was) striving to carve out market share for themselves that can be expected to differentiate themselves from established players by offering consumers more value and benefits. As a result, the newer players can help provide incentives for widespread changes within an entire industry. This effect can be compounded in the face of more negative publicity of the type described above. As companies attempt to reassure consumers, fitting into a well-known paradigm such as a standardized system of privacy settings that is widely known will undoubtedly help a company manage public relations after an embarrassing incident and provide the types of assurances that consumers desire. By fitting into a legislatively mandated system as opposed to a privately branded initiative, businesses must provide consumers with information that would allow them to fully understand what a company is committing to with the force of law behind it. That is to say, by drawing upon an established bundle of pre-defined privacy licenses that can be granted to it by consumers, business can fall in line with consumer expectations without the requirement of having consumers process complex privacy policies that they may not have the patience or the inclination to read. For example, most individuals are able to distinguish between the type of content presented in an R-rated version of a film and a PG-rated version of the same film without incurring the transactions costs involved with doing an in-depth investigation of each film. This same familiarity can work equally well in the information privacy context.

This paper is not attempting to suggest that the system proposed will address any and all concerns that consumers may have with respect to their privacy being respected online. However, it is submitted that a combination of approaches under a Privacy by Design framework will greatly reduce some of the more egregious incidents that contribute to declining consumer confidence in private efforts to respect privacy. Once the major incidents have been significantly curtailed, regulators and industry alike can concentrate their efforts on less high profile, but equally significant lower profile privacy breaches.

CONCLUSION

History has shown that the tradeoff between fostering innovation and providing a stringent regulatory framework to protect consumer privacy has been skewed towards the former. The result is that innovation in the marketplace has come at a cost of a continuing legal uncertainty and turbulence in the marketplace that has damaged the reputation of many online entities. While regulators have been waiting patiently for the market to provide a solution that meets consumer expectations and needs, there are many difficulties with the notice and choice approach that has predominated since the mid 1990's.

Current regulatory developments that emphasize a Privacy by Design approach are a step in the right direction. Rather than relegating privacy concerns subordinate to the needs of technological innovation, this approach builds privacy concerns into the design of new products and services. This approach shows great

141 *Ibid* at 14–16.

promise towards addressing consumer concerns. However, further research needs to be done to see which approaches are the most effective in addressing many of the bargaining issues between businesses and consumers. Commercial and consumer protection law forms an excellent starting point for proponents of the Privacy by Design approach. Rather than approaching problems *de novo*, Privacy by Design advocates can benefit from the experiences of consumer protection advocates in addressing concerns that face contemporary consumers.

It would appear that we have come full circle from the wise words of Warren and Brandeis. Technology has moved at a lightning pace, bringing with it access to information once thought unimaginable. Yet the fundamental rights of individuals to be left alone remain as important today as it was in 1890. The words of Warren and Brandeis are particularly appropriate today since they emphasize that in order to safeguard this right, the law must adapt and keep pace with technology. Otherwise, a further erosion of privacy rights will occur as old problems creep up in new forms. If this fate is to be avoided, the law must remain vigilant to ensure that technology develops in a manner that enhances and does not hinder individual liberty. The approach suggested herein is consistent in the enhancement of individuals' liberty without the unduly onerous or burdensome legal regimes that hinder the efficiency of commercial enterprise.