Socioeconomic and Legal Implications of Electronic Intrusion

Dionysios Politis
Aristotle University of Thessaloniki, Greece

Phaedon Kozyris
Aristotle University of Thessaloniki, Greece

Ioannis Iglezakis
Aristotle University of Thessaloniki, Greece

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Senior Managing Editor: Jamie Snavely
Managing Editor: Jeff Ash
Assistant Managing Editor: Carole Coulson
Typesetter: Sean Woznicki
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue,
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Library of Congress Cataloging-in-Publication Data

Socioeconomic and legal implications of electronic intrusion / Dionysios Politis, Phaedon Kozyris and Ioannis Iglezakis, editors.
p. cm.

Includes bibliographical references and index.
Summary: "This book's goal is to define electronic SPAM and place its legal implications into context for the readers"--Provided by publisher.

ISBN 978-1-60566-204-6 (hardcover) -- ISBN 978-1-60566-205-3 (ebook) 1. Computer crimes--Social aspects. 2. Computer crimes--Law and legislation. 3. Computer networks--Security measures. 4. Consumer protection. 5. SPAM (Electronic mail)--Law and legislation. 6. Privacy, Right of. 7. Identity theft. I. Politis, Dionysios. II. Kozyris, Phaedon J. (Phaedon John) III. Iglezakis, Ioannis, 1965-
HV6773.S635 2009
364.16'8--dc22
2008043297

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter VI
How Much is Too Much?
How Marketing Professionals can Avoid Violating Privacy Laws by Understanding the Privacy Principles

Nicholas P. Robinson
McGill University, Canada

Prescott C. Ensign
Telfer School of Management, University of Ottawa, Canada

ABSTRACT

A marketeer's point of view is presented in this chapter. Although legal restrictions safeguard processes and restrict annoying intrusive techniques, protecting customers, it can be argued that responsible privacy practices in the marketing profession will add value for consumers. As businesses compete with greater intensity to provide the customer with control over areas such as product offerings, services provided, and account management, privacy standards, being an important part of the customer-company relationship, formulate the grounds upon which businesses compete to provide greater customer control.

INTRODUCTION

The numbers were staggering. Over "45 million credit and debit cards, from transactions going back as long ago as 2002" were captured by criminals who had used complex technology to hack into the computer system of Winners – a North American department store chain with numerous outlets in Canada and the United States (Roseman, 2007). The effect, according to a report released by the privacy commissioners of Canada and the province of Alberta was that hundreds of thousands of Canadian and American consumers had their personal data misappropriated and were at risk of identity theft and other related problems (Office of the Privacy Commissioner, 2007).

More worrisomely, the store had not exercised the restraint required by Canada's comprehensive privacy law, the Personal Information Protection and Electronic Documents Act (or "PIPEDA" or the "PIPED Act"), and had unwittingly exacerbated the situation. The company had "collected too much personal information from customers, kept it for too long and relied on weak technology to protect it, according to a joint probe" released by the privacy commissioners (Office of the Privacy Commissioner, 2007). Given events such as the breach at Winners, one can understand the reasons for increased interest in consumer privacy in Canada.

The advent of new technology has made personal data globally mobile and made remote access possible for thieves and fraudsters internationally. In this light, Canada and numerous other nations have enacted privacy legislation to combat the threat of privacy breaches like the one at Winners. The PIPED Act came to force for the public sector in 2001 but has been in force for the private sector since 2004 (PIPEDA, 2000). The legislation, compelled by pressures from the European Union to develop more comprehensive privacy laws, elaborates on a number of principles that private sector businesses must follow and has created methods for recourse by individuals who feel their privacy, known as data protection in Europe, has been violated (European Directive 95/46/EC). The legal implications of electronic intrusion and new privacy laws can be understood as both a threat and an opportunity, as it has increased the cost of acquiring and managing personal information while spurring the creation of marketing practices that are more respectful of consumers' privacy concerns (Robinson & Large, 2004, p. 49).

In fact, it can be argued that responsible privacy practices in the marketing profession will add value for consumers while helping to avoid future breaches, like the one at Winners. The privacy principles elaborated in PIPEDA will both help to protect vulnerable consumers from the threat of electronic intrusion while having a mixed impact on the marketing profession. By examining the three years' worth of available case law, one can understand the costs and benefits of privacy laws and the necessity of privacy legislation in light of electronic threats. Indeed, privacy will be one of the defining human rights issues of the 21st century given that technological advances and the increased disclosure of personal information will make those who control personal information, namely businesses and governments, increasingly powerful. The marketing profession will play a pivotal role in democratizing privacy rights and discouraging electronic intrusion by actively supporting privacy legislation and other government endeavours to protect the citizen's privacy interests (NB: An implied right to privacy exists in Canada and many other countries (Canadian Charter of Rights, 1982, s.7)).

BACKGROUND: THE PRIVACY PRINCIPLES IN ACTION

The privacy principles elaborated in PIPEDA serve as a guide to businesses and others who are subject to the Act. The privacy principles apply to all personal information that is "collected, used, or disclosed by an organization in the private sector" (Tacit, 2003, p.1). Personal information, according to the Canadian Act, includes information about any "identifiable individual, other than an individual's name, title, business address or telephone number as an employee of an organization" (Tacit, 2003, p.1). Exceptions are included for artistic and journalistic pursuits, and other areas of public interest where privacy law could be prohibitive to a socially beneficial activity (Tacit, 2003, p.3).

Those who are subject to PIPEDA must therefore attempt to develop business practices that are consistent with the Act's spirit. The privacy principles, developed by the Canadian Standards Association and inspired by a similar set of OECD principles, include: (1) limiting collection,

(2) accuracy and completeness, (3) identifying purposes, (4) consent, (5) limiting use retention and disclosure, (6) safeguards, (7) openness, (8) challenging compliance, (9) access, and (10) accountability (PIPEDA, 2000, Schedule 1 s. 5). These principles are designed to be interpreted according to the particular scenario and cannot be uniformly applied given the particularities of the uses of personal data, the subject of the data, and the overall scenario.

The first of the ten privacy principles, accountability, requires that all organizations that are subject to the law, large and small, designate someone who is "accountable for the organization's compliance with the …principles" (PIPEDA, 2000, s. 5 (4.1)). Though the management of personal information may be delegated to others, the designated individual must ensure that the organization has the policies and practices necessary to ensure compliance. All "personal information in its possession or custody, including information that has been transferred to a third party for processing" is covered by this definition (PIPEDA, 2000, s.5 (4.1.3)). The principle of accountability, as with all other principles, is interdependent and supports an individual claimant's ability to challenge the organization's compliance. From a marketing standpoint, this implies that marketing professionals will have to give deference to privacy concerns, and give deference to the designated individual, in order to ensure campaigns are compliant. This is of special importance when personal data is transmitted and shared in order to produce an effective marketing campaign. The designated compliance officer in charge of ensuring accountability would oversee activities involving sales lists and customer data.

Marketers are also required to identify the purposes of the information being collected "at or before" it is collected (PIPEDA, 2000, s.5 (4.2)). This adds an additional layer of administration when surveys and other market research activities are being undertaken, as participants must be informed of the reasons for the collection of information and its uses. Further, the information being collected must have a logical nexus with the purpose identified—in other words, it must be "necessary" to achieve the identified purpose (PIPEDA, 2000, s. 5 (4.2.2)). In the case Eastmond v. Canadian Pacific Railway, where a video camera was installed in a rail yard, the court deemed the purpose of encouraging workplace safety and protecting company machinery from vandalism and theft acceptable (Eastmond v. CPR, 2004, para. 178). The court went even further by stating that every purpose must be "analysed in a contextual manner" giving weight to the "particular circumstances" and suggested that the purpose of collecting the information, and the purpose of disclosing the information need not be identical (Eastmond v. CPR, 2004, para. 131). This principle implies that marketers can no longer arbitrarily use information collected for one purpose and then for another purpose later on, unless the original participants are informed of the new purpose (Eastmond v. CPR, 2004, para. 178). Further, the flexibility that market researchers once had in using information to for new purposes is compromised and collecting information that has no immediate nexus with the proposed purpose is forbidden.

The purposes identified by the organization must be consented to along with the particular uses named and any disclosures of the personal information to other parties. Consent, the third privacy principle, is "required for the collection of personal information and the subsequent use or disclosure of this information" (PIPEDA, 2000, s.5 (4.3.1)). Consent can be obtained orally, implicitly through one's use of a product or service, and through written documents, such as an application form or a check-off box. In jurisprudence, application forms describing the reason for obtaining biometric data (opt-in consent) and signs indicating the presence of video surveillance systems (opt-out consent) have been considered valid forms of consent (Turner v. Telus Communications, 2005; Eastmond v. CPR, 2004).

Further, in instances where consent would make the achievement of the purpose impossible or difficult, explicit consent may not have to be sought (Eastmond v. CPR, 2004, p. 186). In Turner v. Telus, an application form to collect biometric data (including a voice imprint) was considered sufficient consent (Turner v. Telus, 2005, para. 58). A minority of employees refused consent in this case, without any repercussions from Telus, making this case an example of how privacy laws empower individual citizens to protect their privacy interests. For the marketing profession, being unable to obtain consent may stand as a barrier to certain research projects.

However, the barrier posed by the consent requirement advances several other goals that all pieces of privacy legislation aim to achieve. For instance, limiting the collection of information and empowering the consumer to take control over his or her personal data. All privacy laws aim to limit the collection of information by organizations in order to lessen the chances of abusive use of personal information and privacy breaches, as in the Winners case. Limiting collection, the fourth privacy principle, is interdependent with many of the other principles. For instance, collection can be limited on the basis that information may only be collected for a particular purpose, and likewise, with the consent of the individual. The information collected should be "limited to that which is necessary for the purposes identified by the organization", both in terms of the "type and the amount" of information collected (PIPEDA, 2000, s. 5 (4.4)). Further, the Act states that information should not be collected "indiscriminately" (PIPEDA, 2000, s. 5 (4.4.1)). The electronic disclosure of personal information by the Bank of Nova Scotia to the Royal Bank of Canada for a purpose other than the purpose the individual customer consented to at the time of collection has been deemed to be inconsistent with PIPEDA (B.M.P. Global Distribution v. Bank of Nova Scotia, 2005). When information is collected, it can only be disclosed for the purposes specified and consented to by the individual in question, with some exceptions for certain groups like investigative bodies. Likewise, cameras geared to observe only those entering and leaving CPR company facilities were deemed to have been consistent with the principle of limiting collection (Eastmond v. CPR, 2004, para. 178). Data mining activities that arbitrarily (and indiscriminately) collect consumer information, as with cookies and other electronic tools used to gather information on target customers, likely would not meet the standards of limiting collection. Thus, it can be said that the principle of limiting collection restricts many marketing practices.

Limiting collection is also related to the fifth principle, limiting use, retention and disclosure. This principles states that personal information should be "retained only as long as necessary for the fulfilment of those purposes" and can only be used or disclosed in a manner that is consistent with the purpose identified and consented to (PIPEDA, 2000, s. 5 (4.5)). Further, to discourage the propagation of personal information subject to privacy concerns, the principle of limiting use, retention and disclosure requires that information that is no longer necessary to serve the original purpose be "destroyed, erased, or made anonymous" (PIPEDA, 2000, s. 5 (4.5.3)). In the case Eastmond v. CPR, the court ruled that CPR had implemented practices that were consistent with limiting retention and disclosure. The company kept video captured by cameras for 92-hour periods and the video was only viewed if a "trigger" incident, such as a theft or another incident, occurred (Eastmond v. CPR, 2004, para. 138). Further, the video was kept under lock and key and disclosure was only made available to company officials and police (Eastmond v. CPR, 2004, para. 178). Conversely, the Bank of Nova Scotia's disclosure of information about a counterfeit cheque to the Royal Bank was deemed to run counter to the principle of limiting disclosure as the disclosure was not consented to by the customer and not captured under any of the Acts

exceptions for disclosure without consent. The privacy principles therefore limit subsequent uses of private information, even for compelling business purposes, and curtail the marketer's ability to freely manage and use data.

The sixth privacy principle, accuracy, states that information should be "accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used" (PIPEDA, 2000, s. 5 (4.6)). The individual's right to access the information and request that errors and omissions be corrected supports this obligation. In fact, courts have interpreted the accuracy principle as meaning that the customer can compel the organization to correct information, not that the organization is responsible for ensuring "that records kept by private organizations be inalterable or that their integrity be guaranteed" (PIPEDA, 2000, s. 5 (4.6)). In the case Vandebeke v. Royal Bank of Canada, a client's incomplete and supposedly inaccurate bank records caused a prejudice (Vandebeke v. RBC, 2006). The court stated that the bank's responsibility was limited to ensuring that the customer could rectify problems with his information (Vandebeke v. RBC, 2006, para. 22). From the perspective of a marketing professional, securely maintaining information is an onerous task in itself. It would be difficult to assure the complete accuracy of information, especially when an organization is not at fault for the inaccuracy or incompleteness of information. Privacy laws therefore strikes a balance between the rights of the individual and the abilities of the organization and establishes an effective regime for the self-monitoring of an individual's data.

The seventh privacy principle, security safeguards, is interdependent with the sixth principle, as safeguards are needed to ensure accuracy and protect data from tampering. In order to ensure accuracy, "security safeguards appropriate to the sensitivity of the information" must be taken using physical, organizational and technological measures to protect the data (PIPEDA, 2000, s. 5 (4.7)). This means that the level of protection provided should be commensurate with the nature and amount of information stored. The safeguards employed by Winners, for instance, were deemed to have been incommensurate with the sensitivity of the credit card information that was stolen (Roseman, 2007). In Turner v. Telus, the court stated that a proactive approach to protecting personal data is necessary to ensure that safeguards are in place (Turner v. Telus, 2005, para. 22). The company's use of biometric employee data, though potentially harmful to the employee's privacy, was deemed important to protecting the customer's privacy. Safeguards are important in ensuring that the information used is of good quality, and therefore mutually benefit both the individual and the marketing professional applying the information.

Openness is also necessary to encourage self-enforcement by individual consumers and others. Openness, the eighth principle, means that the organization should make "readily available to individuals specific information about its policies and practices relating to the management of personal information" (PIPEDA, 2000, s. 5 (4.8)). Information on policies, practices, and those designated as accountable for the company's compliance facilitates access to information makes it easier for individuals to challenge compliance. Being open with regards to the management of information by a company complicates the role of the marketing professional, as one must ensure that they comply with internal policies while communicating how the information in question is being managed. The openness principle increases the burden of responsibility on the marketing professional and therefore encourages practices that are respectful of an individual's privacy rights. For precisely this reason, in the case Thomas v. Robinson the company sought a declaration that the databases it managed were excluded under privacy legislation in the province of Ontario (Thomas v. Robinson, 2001). Openness runs counter to protecting sensitive information and represents a cost when a company wishes to conceal its operations from

the public—especially considering the burden that may be posed by outside interference in marketing activities. This being said, openness is also essential to ensuring the consumer's right to privacy is protected.

The ninth principle, access, requires that an organization inform an individual "of the existence, use, and disclosure of his or her personal information and shall be given access to that information" upon request (PIPEDA, 2000, s. 5 (4.9)). Further, the individual has a right to request that the information be complete and accurate and have necessary corrections made. The information must be furnished to the individual within a "reasonable time" and may often be subject to a fee, in order to cover the costs of furnishing the information (PIPEDA, 2000, s. 5 (4.9)). In the case Rousseau v. Wyndowe, the court ruled that an individual had no right to access original notes made by a medical professional where the exact same material could be accessed through electronic records (Rousseau v. Wyndowe, 2006). Providing access through an electronic database was deemed to be sufficient where paper copies had been destroyed. In some circumstances, the Act states that outright denying access to documentation of personal information is permitted.

The last privacy principle, challenging compliance, states that an individual should be able to "address a challenge concerning compliance with the above principles to the designated individual" accountable for an organization's compliance (PIPEDA, 2000, s. 5 (4.10)). In other words, the organization has a responsibility to facilitate the individual's complaint by "informing individuals" of the relevant procedures and options they have to pursue the complaint (PIPEDA, 2000, s. 5 (4.10)). The principle of challenging compliance is closely related with the principles of access and openness and can only function where these other two principles exist. Further, compliance with the law can be challenged through complaints to government appointed privacy officers who are responsible for administering complaints and inquiries regarding each jurisdiction's respective legislation. Many jurisdictions in Europe and elsewhere have privacy commissioners who facilitate complaints and monitor compliance. The ability of the individual to challenge compliance adds impetus for marketing professionals to follow the privacy principles given that the repercussions of non-compliance can be costly.

Though this ordering of the privacy principles is Canadian by definition, other organizations (particularly in Europe) have produced their own principles that are nearly identical to the Canadian principles. For instance, the OECD principles include use limitation, collection limitation, data quality, purpose specification, security safeguards, openness, individual participation, and accountability (OECD, 2007). These principles are also reflected in several EU directives, some of which have had the practical effect of forcing third party data users in countries like Canada to comply with European privacy standards. In this light, PIPEDA and other schemes such as the US Safe Harbor Agreement are responses to the EU directive and are "substantially similar" to the European standards (EC Directive 95/46/EC, 1995). In fact, the Canadian privacy principles and PIPEDA itself are mirror reflections of the EU standards and the OECD principles. This being said, unlike Canada, the United States opted to find a non-legislative solution to meeting the EU's demands that European data transferred abroad be treated in a manner that adequately meets EU privacy standards, something that has been advocated by business groups in the United States (Kutais, 2007, p. 60). The end product, the US Safe Harbor agreement is an opt-in program for US companies that transfer data between Europe and the United States and requires participating companies to comply with fixed privacy standards (Government of the United States, 2007). In addition to any guarantees created by the US Safe Harbor agreement, European nationals and others have access to judicial recourse against US companies that abusively violate a consumer's

privacy through conventional court actions. US companies may be held liable for injuries caused by privacy violations through tort law and are subject to numerous other pieces of legislation that limits their use of personal information.

MAIN THRUST: ELECTRONIC INTRUSION AND PROTECTING THE CONSUMER

Issues

We know that one of the great conundrums of e-business is that it gives enterprises a powerful new capability to capture and analyze massive amounts of customer information so they can serve individuals more effectively. Yet this very capability troubles some people, who see it as a means to disclose or exploit their personal information. These are legitimate concerns, and they must be addressed if the world of e-business is to reach its full potential. At its core, privacy is not a technology issue; it is a policy issue. And the policy framework that's needed here must involve the technology industry, the private sector in general, and public officials. November 2001, IBM Chairman, Louis Gerstner, Jr. (Privacy Guru Joins IBM, 2001, p. 1).

IBM Chairman Louis Gerstner Jr., like many other business leaders, recognizes the enormous potential and threat that new technology poses. The rise of countless new ICTs ("information communications technologies") has meant that marketers can better serve consumers and marketers have greater power to use, and even abuse, private information. Electronic tracking systems, cookies, spy ware, and spam are all realities of the modern Internet age. They are also examples of how the Internet has opened up new avenues to sell products and collect data. This being said, privacy law serves the important purpose of curbing the negative impact of some of these intrusive techniques and delineating when their use is acceptable.

Some of these intrusive techniques are, by definition, nuisances to consumers. Spam, which can be defined as "unsolicited commercial email (UCE) or junk mail", is a commonly cited problem for many Internet users who find their private information being collected and sourced to companies interested in promoting their wares (Kutais, 2007, p. 60). Sophos Research has found that the United States is the world's biggest spam producer (at 56.7%), followed by other members of the so called "dirty dozen" including Canada at 6.8%, China at 6.2%, Brazil at 2%, and France, Germany, Spain, and the UK at between 1% and 2% (Sophos Research, 2007). Though there may be civil and even criminal liability for mass spam operations, several other forms of electronic intrusion have traditionally posed a greater threat to consumer privacy and business interests. In the United States and many other countries, for example, actions that violate the privacy principles may be criminally punishable. For instance, the US Computer Fraud and Abuse Act (CFAA), 18 USC ss. 1030 states that data manipulation, which involves corrupting existing information, is a criminal offence (US Computer Fraud and Abuse Act). Data manipulation relates directly to the principle of data accuracy in privacy law, which stresses the consumer's right to have their personal data corrected for accuracy. Further, it places the onus on private sector organizations and marketers to ensure data is safely protected, as intruders can manipulate customer data leaving the company liable.

Perhaps the most troubling form of electronic intrusion involves the use of spy ware and other electronic tools to collect private information. As in Winners, hackers will often integrate electronic tools into existing computer systems in order to expropriate personal data such as credit card information. In the United States, several pieces of existing and proposed legislation attempt to address the overwhelming problem of unauthor-

ized electronic collection of personal data. The Children's Online Privacy Protection Act sets rules for the collection of information concerning children under the age of 13 via websites, most notably by requiring parental consent to obtain information (Kutais, 2007, p. 59 & 63).

Further, legislation has been proposed by the 108th US Congress to impose sweeping provisions regulating consumer privacy for all US citizens (Kutais, 2007). The Consumer Privacy Protection Act is a comprehensive piece of legislation that is remarkably similar to Canadian and European privacy laws, and substantially embraces the same principles, though still employing a self-regulatory framework (Kutais, 2007, p. 63). In addition, four bills that deal specifically with the issue of Internet spy ware are pending approval (Kutais, 2007, p. 72). The SPY ACT, an acronym for Securely Protect Yourself Against Cyber Trespass, would make it unlawful for anyone to "collect personally identifiable information through key logging" and other means, and would prohibit the collection of certain types of information without consent (Kutais, 2007, p. 72). The Spy Act also contains numerous provisions related to tampering with elements of a computer's software for the purpose of collecting information, such as the installation of a spy ware device or the modification of computer settings (Kutais, 2007, p. 72-73). Opponents to this legislation and other pieces of legislation have argued "not to preclude the evolution of tools and marketplace solutions to the problem" of electronic intrusion and spy ware (Kutais, 2007, p. 75). This argument is a valid one, and, at that, one that has been made in a number of different contexts. For instance, in a similar vein, while the United States was negotiating the Safe Harbour Agreement with the EU a US lobbyist made the argument that had a legislative solution been implemented to protect consumer privacy 100 years earlier modern credit reporting may never have evolved (Robinson & Large, 2004, p. 10). Freedom of information is paradoxically as important as protecting privacy, given that information enables debate and dynamism—both of which capitalism needs to thrive.

The American approach to privacy can therefore be viewed as far less paternalistic than the Canadian or European approaches that aim to protect unsophisticated and vulnerable individuals from privacy breaches (Politis, 2001, pp. 258-267). Though non-legislative solutions may work for savvy internet users who wish to be able to "have control over whom they shared that information with" (in the words of FaceBook founder Mark Zuckerberg), failing legislation many individuals may be uncertain about their rights and fall prey to intrusive data collection practices (Stinchcombe, 2006). In this sense, it can be argued that privacy law should empower the consumer to have control while protecting those who are potentially vulnerable. Discounting explicit breaches of consumer privacy, such as the one at Winners, statistics indicate that in the United States alone "one in four credit reports contain errors serious enough to disqualify consumers from buying a home, opening a bank account, or getting a job" (The Direct Marketing Association, 2007).

Arguably, facts like this should be troubling enough to spur on greater powers for consumers who wish to guard their privacy. Marketers as well have argued that healthy privacy practices are beneficial to consumer relations and can have a positive business impact, despite the administrative overhead. Satisfied customers, it is argued, "return to the organization that has treated them well in the past" and will appreciate privacy practices that meet the consumer's expectations (Gilbert, 2002, p. 6 as cited in Robinson & Large, 2004, p.3). This being said, the consumer's desire for privacy and desire for "customized" or individual treatment are "inherently contradictory" (Trott & Jones, 2001, p. 1 & 12). Weak privacy standards make the indiscriminate collection of information possible and allow companies to deliver better solutions, both in marketing and in sales, to customers (Trott & Jones, 2001, p. 1 & 12). This means that respecting the privacy

principles by employing ethical consumer-driven uses of technology can both improve customer relations and make it more difficult for a firm to devise novel solutions to consumer needs.

Solutions

According to numerous scholars, the customer's faith in the company and its privacy practices will dictate whether the customer chooses to engage in further transactions with the business. One scholar states that online trust is "a key differentiator that determines the success or failure of many companies conducting their business over the Internet" (Lauer & Deng, 2007, p. 323). Similarly, others note that customer and employee demands cannot be "realized without suitable privacy, security, and trust technologies to ensure that business data is appropriately protected and business partners can inter-work with confidence" (Knight, Buffet, & Hung, 2007, p. 285). Moreover, privacy is identified as just one of the many ways that a company can enhance trust (Lauer & Deng, 2007, p. 323). Trust can be "enhanced through two complementary approaches: secured information technology and trusted business practices" (Lauer & Deng, 2007, p. 323). Privacy practices are therefore critical to the firm's long-term relationship with clients and even employees and respecting privacy laws and the consumer's privacy interests should be at the forefront of every CEO's mind (Lauer & Deng, 2007, p. 323). One scholar's research has concluded that a stronger privacy policy means "higher perceived trust-worthiness" and "higher perceived trustworthiness leads to greater trust" (Lauer & Deng, 2007, p. 329). In turn, "greater customer trust results in a higher level of customer truthfulness" as well as "greater customer loyalty" (Lauer & Deng, 2007, p. 329). According to Lauer and Deng (2007, p. 329) the perceived integrity, benevolence and ability of the business is determinative of the extent to which the consumer trusts the business with his or her personal information, and the level of vulnerability the customer is willing to accept. According to the model espoused, "to trust another party, a trustor must perceive that the trustee has the ability to do good to the trustor in the relationship, and adheres to a set of principles that the trustor finds acceptable" (Lauer & Deng, 2007, p. 325). This idea has been corroborated by Ensign (2002, p. 136), who found that reputation, based both on past history and expectations for future actions, is influential in determining whether an individual would share knowledge in an office environment.

With regards to consumer-business relations, trust is a critical factor that has both costs and benefits. Many companies have enacted "fair information practices" on the basis of "ethical imperatives or on faith that an ethical stance will lead to business benefits down the road" while accepting that this action may also mean foregoing practices that have short-term pecuniary benefits and are less respectful of consumer privacy (Lauer & Deng, 2007, p. 330). The example of the sale of customer data, which would be in clear violation of the disclosure principle if not undertaken with the consent of the individual concerned, is given (Lauer & Deng, 2007, p. 330). These authors also note "the most desirable customers, those with discretionary income and higher levels of education, are often the most privacy aware" (Lauer & Deng, 2007, p. 330). Further, a solid privacy policy can protect a firm from the embarrassment faced by companies such as Winners that had weak practices in place. A "strong privacy policy can serve as insurance against privacy disasters where customer data is exposed and a company may experience loss of reputation and a decline in stock value" (Lauer & Deng, 2007, p. 330). For this reason, it is critical that companies design privacy policies that embrace the privacy principles and then act on these policies by implementing technological and procedural controls that are sufficient to achieve the standards set by the policy.

An adequate privacy policy should include provisions that address all the privacy princi-

ples—namely, collection limitation, accuracy and completeness, identifying purposes, consent, limiting disclosure/use/retention, safeguards, openness, challenging compliance, accountability and access. Further, by obtaining the certification of a recognized independent Internet privacy watchdog, such as TrustE (www.truste.org). These organizations are act as non-governmental watchdogs and are especially popular in the United State where privacy laws are more of a patchwork than other countries, like Canada or Europe. In order to qualify for the certification, the company must have policies and practices in place that meet TrustE's standards. For instance, Microsoft's online privacy statement provides a good example of how the privacy principles can be put into action. In fact, a privacy policy itself exemplifies the principle of openness by creating a dialogue between consumers and the company.

Microsoft's privacy policy identifies and defines the range of information that the company collects online—"We may also collect demographic information, such as your ZIP code, age, gender, preferences, interests and favorites" (Microsoft, 2007). Greater specificity strengthens the policy but may put a damper on the company's ability to act with flexibility (Microsoft, 2007).

Microsoft also takes a customer-driven approach to privacy, placing part of the burden of accuracy largely on the consumer or the source of the information in question (Microsoft, 2007). This being said, accuracy and completeness is a collective effort requiring both the consumer and the company to review records. Microsoft also identifies the purposes for which it collects information. Information is collected and used to "create a Microsoft billing account", to "offer you a more consistent and personalized experience in your interactions with Microsoft", and to provide "more effective customer service" (Microsoft, 2007). Opt-out consent, meaning that consent is assumed, is used for parts of the privacy policy placing the burden on the consumer to indicate that their information should not be used (Microsoft, 2007). Opt-in consent, which is used less frequently on the Internet given the logistical difficulty in obtaining this form of consent, is generally believed to create a stronger privacy policy given that the consumer must acknowledge and agree to the collection and use of the information. Further, the company reveals the limits of the use and disclosure of the information it collects, identifying the subsidiaries and business functions that have access to the information. The company also identifies the safety precautions, both technological and procedural, that it takes to protect personal data (Microsoft, 2007). Safeguards such as "unique ID" numbers, "encryption, such as the Secure Socket Layer (SSL) Protocol", and others are identified (Microsoft, 2007). Microsoft offers its online users and customers with options for pursuing concerns and complaints (i.e. challenging compliance), directing the consumer to the TrustE website & dispute resolution procedure (i.e. accountability) and a contact point at Microsoft (Microsoft, 2007). Further, the website also indicates the company's participation in the US Safe Harbor Agreement (with the EU in accordance with EU Directive 95/46/EC) (Microsoft, 2007). Lastly, Microsoft identifies means by which the consumer can access his or her personal information. Information that is not immediately available can be requested by contacting the company (Microsoft, 2007).

Reinforcing a solid privacy policy, such as the one available on the Microsoft website, with procedures, practices, and technologies that adequately meet the firm's commitments will go a long way in ensuring compliance with privacy laws. Further, having such a policy in place makes sense given the importance of privacy issues to consumers and the company's legal obligation to protect the consumer's privacy interests. Microsoft's policy exemplifies the universality of the privacy principles used in the Canadian PIPED Act and reflected in the OECD privacy principles and the EU Directive. Creating and applying policies that are consistent with these principles

will be critical for companies that wish to retain customers and avoid the embarrassment of a serious privacy breach such as the one experienced by Winners.

FUTURE TRENDS

A suitable privacy policy alone, however, is not sufficient for businesses that wish to go beyond simply satisfying the customer's privacy needs and abiding by the law. Companies that wish to both meet the demands of customers and legislators for better privacy standards while using privacy to improve client-company relations must view privacy as a tool that the customer can control. Frederick Newell, in his book *Why CRM Doesn't Work,* argues for increased customer influence when it comes to managing the client-company relationship (Newell, 2003, p. 5). This becomes particularly important for marketing professionals as better customer relations often means a better bottom line. More specifically, future trends would seem to indicate that businesses will compete with greater intensity to provide the customer with control over areas such as product offerings, services provided, and account management. Privacy standards, being an important part of the customer-company relationship, will be one of the grounds upon which businesses compete to provide greater customer control. In other words, companies that can empower customers to have control over their personal information will be able to develop better relationships with them.

In the future, this may represent an important basis for competition and could make the development and implementation of customer friendly technologies critical. It is therefore no wonder why most e-businesses, from facebook to ebay, enable customers to modify and alter their personal profiles and other information that could compromise privacy. The movement of this trend from the online sphere to all forms of electronic commerce will continue, thereby better enabling customers to protect themselves from electronic intruders and manage their personal data. According to Newell, "customers, not companies, control the purchasing process today by having access to more information, and having it in real time…the Internet has given them unprecedented research tools" (Newell, 2003, p. 6). Innovative software that allows customers to better manage their private data will accelerate this process and give customers greater control. In this light, future research on the impact that "customer management of relationships" has on electronic intrusion and the profitability of customer-company business relations is merited (Newell, 2003, p. 167).

CONCLUSION

Big Brother is Watching You!

(Orwell, 1949)

In George Orwell's classic novel Nineteen Eighty-Four, the author portrays life in the modern era as defined by constant surveillance and scarce privacy. Eerily, the spirit of Orwell's novel may be more relevant today than ever before given advances in technology and our increasing willingness to share information. Indeed, today more than ever before, legislators need to address issues surrounding privacy, as personal information has become a tool that can be both used to undertake criminal acts and better meet consumer needs. In this light, privacy legislation in Canada, Europe and the United States will play a particularly important role in the electronic era. Demarcating how technology can be employed to collect, use, manage and disclose information will be a critical first step in ensuring that consumers are capable of protecting themselves. This being said, new privacy laws have implications for the business community and will lead to increased bureaucracy and create potential legal liability for those that fail to comply. By understanding the spirit of the privacy principles and undertaking

to meet the consumers' need for control over personal data businesses can avoid privacy breaches and foster healthy relationships with customers. Marketers, and business people more generally, can benefit from practices and policies that live out the objectives of the privacy principles. Collection limitation, accuracy and completeness, identifying purposes, consent, limiting disclosure/use/retention, safeguards, openness, challenging compliance, accountability and access represent the key pieces of the privacy puzzle that must be implemented collectively in order to meet the legal standards enshrined in privacy laws internationally and gain the trust of consumers. Implementing a privacy policy, like the one used by Microsoft, that incorporates the privacy principles will help to protect vulnerable consumers from electronic intrusions, such as the event at Winners, while having a mixed impact on the marketing profession. Better relationships with consumers may also mean more costly marketing practices and increased investments in customer privacy. Considering the risks posed by electronic privacy breaches, ranging from identity theft to financial liability, it is more imperative than ever before that governments, companies and individuals act to protect the private citizen's "right to be let alone" (Warren & Brandeis, 1890).

REFERENCES

Privacy guru joins IBM. (November 30, 2001). Retrieved March 10, 2004, from http://www.crm-forum.com

B. M. P. Global Distribution Inc. v. Bank of Nova Scotia (c.o.b. Scotiabank), B.C.J. No. 1662.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *i*(5).

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being, Schedule B to the Canada Act 1982 (U.K.), 1982, c.11 s. 7.

Canadian Standards Association. (November 19, 2007). *CSA Model Code for Privacy Protection*. Retrieved November 20, 2007, from http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=English

Direct Marketing Association. (November 19, 2007). *Survey: 1 in 4 Credit Reports Contain Errors*. Retrieved November 19, 2007, from http://www.thedma.org/cgi/dispnewsstand?article=2440

Eastmond v. Canadian Pacific Railway. [2004]. F.C.J. No. 1043.

EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

Prescott, E. C. (2002). *Reputation and technological knowledge sharing among R&D scientists in the multidivisional, multinational firm*. Montreal: Univeristy of Montreal, Unpublished Dissertation.

Government of the United States. (2004). *US Safe Harbor Agreement*. Retrieved November 19, 2007, from http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm

Knight, S., Buffett, S., & Hung, Patrick C.K. (2007). Guest Editors' Introduction. *International Journal of Information*, *6*(5), 285-286.

Kutais, B. G. (Ed.) (2007). *Spam and Internet Privacy*. New York: Nova Science Publishers.

Lauer, T. W., & Xiaodong, D. (2007). Building online trust through privacy practices. *International Journal of Information Security*, *6*(5), 323-331.

Microsoft. (2008). Retrieved November 19, 2007, from http://privacy.microsoft.com/en-us/fullnotice.aspx

Newell, F. (2003). *Why CRM Doesn't Work: How to win by letting customers manage the relationship*. Princeton, NJ: Bloomberg Press.

OECD. (2002). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved November 19, 2007, from http://www1.oecd.org/publications/e-book/9302011e.pdf

Office of the Privacy Commissioner of Canada. (2007). *Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies Inc./Winners Merchant International L.P.* Retrieved November 19, 2007, from http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp

Orwell, G. (1949). *Nineteen Eighty-Four*. London: Martin Secker and Warburg.

Personal Information and Electronics Document Act, R.S.C. 2000, c.6.

Politis, D. & Gogos, K. (2001). Data mining of Personal Information: Perspectives and Legal Barriers. Proceedings of the *5th wses/IEEE World Multiconference on Circuits, Systems, Communications & Computers. CSCC 2001*, Rethymnon, Crete, 8-15 July 2001, (pp. 258-267).

Robinson, N., & Large, D. (2004, December). PIPEDA: Impact on CRM and public-private sector interaction. *Optimum Online: The Journal of Public Sector Management*, *34*(4), 47-60.

Roseman, E. (2007). How retailers can protect customer privacy. *The Toronto Star* (7 October 2007).

Rousseau v. Wyndowe, [2006] F.C.J. No. 1631.

Sophos Research. (2007). *The Dirty Dozen*. Retrieved November 11, 2007, from http://www.sophos.com/pressoffice/news/articles/2004/02/sa_dirtydozen.html

Stinchcombe, K. (September 25, 2006). Facebook privacy. *The Stanford Daily* (25 September 2006). Retrieved November 18, 2007, from http://daily.stanford.edu/article/2006/9/25/facebookPrivacy

Tacit, C. (2003). Complying with private sector privacy legislation (Unpublished Work).

Thomas v. Robinson, [2001] O.J. No. 4373.

Trott, B., & Jones, J. (April 2, 2001). Industry tows the privacy-CRM line. *InfoWorld*. Retrieved March 11, 2004, from www.infoworld.com

TrustE. (2008). Retrieved January 6, 2008, from http://www.truste.org/about/index.php

Turner v. Telus Communications, [2005] F.C.J. No. 1981.

US Computer Fraud and Abuse Act (CFAA), 18 USC ss 1030.

Vanderbeke v. Royal Bank of Canada, [2006] F.C.J. No. 871.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5).

ADDITIONAL READING

Alderman, E., & Kennedy, C. (1997). *The Right to Privacy.* New York: Vintage.

Papazoglou, M., & Ribbers, P. (2006). *E-Business – Organizational and Technical Foundations.* West Sussex, UK: Wiley.

Solove, D. J., Rotenberg, M., & Schwartz, P. M. (2006). *Information Privacy Law.* New York: Aspen Publishers.

KEY TERMS

Customer Relationship Management ("CRM"): Management practices that aim to better satisfy customer needs by seeking to understand those customer needs and build a lasting relationship with the consumer. Personal information, and therefore privacy issues, is critical to any CRM plan.

Data Mining: The arbitrary and often indiscriminate collection of personal data for the purposes of improving marketing efforts and sometimes criminality. Data Mining most often utilizes the Internet and other electronic means but can include more traditional methods of collecting information.

Electronic Intrusion: The invasion of Internet privacy through spy ware, hacking, Spam, and other electronic technologies. Electronic intrusion is a serious concern for internet-users and privacy commissions alike which have increasingly begun to look at legislative solutions to this pressing threat to consumer privacy.

PIPEDA or PIPED Act: The "Personal Information Protection and Electronic Documents Act" is a recent piece of Canadian privacy legislation that aims to empower Canadian consumers in protecting their privacy. PIPEDA, a law inspired by the CSA and OECD principles and various EU Directives, requires all Canadian businesses to follow strict privacy practices in regards to all personal data.

Privacy Policy: The collection of technological, commercial, and legal issues surrounding the protection of the right to privacy. Privacy policy encompasses and affects many different interconnected policy areas and hinges on the question of the extend to which the individual has a right to be free from outside interference.

Privacy Principles: These principles (developed by the CSA) are intended to guide organizations in developing practices that are respectful of privacy rights. They include (1) limiting collection, (2) accuracy and completeness, (3) identifying purposes, (4) consent, (5) limiting use retention and disclosure, (6) safeguards, (7) openness, (8) challenging compliance, (9) access, and (10) accountability. The Canadian Standards Association developed these principles and they are an important part of the PIPED Act.