DATA BREACHES: WORTH NOTICING?

Written By: John Lawford and Janet Lo
Additional writing and research: Laman Meshadiyeva and Roxane Gunning
Public Interest Advocacy Centre
1204 – ONE Nicholas St
Ottawa, Ontario
K1N 7B7

December 2011

Published January 2012

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, Ontario
K1N 7B7

Canadian Cataloguing and Publication Data

Data Breaches: Worth Noticing?

ISBN

1-895060-63-X

PIAC received funding from Industry Canada's Contributions Program for Non-Profit Consumer and Voluntary Organizations to prepare the report. The views expressed in the report are not necessarily those of Industry Canada or the Government of Canada.

Executive Summary

This report examines data breach notification in Canada in the private sector in general and in particular whether the proposed federal data breach notification law, *An Act to amend the Personal Information Protection and Electronic Documents Act* (Bill C-12), is adequate to protect Canadian consumers.

"Data breaches" are a loss, unauthorized access to or unauthorized disclosure of individuals' personal information by an organization holding that data. At present, only Alberta law requires reporting of private sector data breaches. Federally, such data breaches presently are covered by voluntary guidelines from the Privacy Commissioner of Canada.

The report concludes that the proposed data breach notification requirements in Bill C-12 grant excessive discretion to organizations that have had a data breach, allowing them unilaterally to characterize the breach as non-harmful to consumers. In so doing, organizations gain the benefit of a largely unreviewable decision in the face of a manifest and undeniable conflict of interest. The result is likely to be a vast underreporting of serious data breaches, which puts consumer welfare at excessive risk.

Therefore, PIAC supports an "Alberta model modified" data breach law at the federal level.

Recommendations include the following legislative changes (as amendments to Bill C-12 or additions or amendments to provincial legislation):

1. **There should be a duty to report all data breaches to the relevant privacy commissioner, either "as soon as reasonably possible" or within a short time window such as 48 hours;**
2. **There should be clear monetary penalties for not reporting to the privacy commissioner;**
3. **The privacy commissioner should decide on customer notification, based on a harm test. This test should be objective and based on the standard of "real risk of significant harm";**
4. **The privacy commissioner should be given the power to order an organization to report a breach to customers. Orders to notify customers should be made public as should the name of the organization involved;**
5. **The privacy commissioner should have adequate audit powers to examine corporate data security practices and in particular to examine an organization's data breach notification preparedness and response;**
6. **The adequacy and effectiveness of the data breach regime should be separately evaluated at the time of the next review of PIPEDA or provincial privacy legislation.**

In addition, consideration should be given to the following recommendations independent of the legislative framework for breach notification:

7. **The privacy commissioner should create a dedicated data breach division, with adequate staffing, to address only data breaches.**
8. **The privacy commissioner should convene a "data breach advisory board" to bring current corporate information security expertise, consumer protection expertise and government regulatory expertise to bear on the question of data breaches.**
9. **The privacy commissioner should take a lead role in informing Canadians of how breach notification works, including a dedicated web page and online resources.**

Acknowledgement

The Public Interest Advocacy Centre received funding from Industry Canada's Contributions Program for Non-profit Consumer and Voluntary Organizations. The views expressed in this report are not necessarily those of Industry Canada or of the Government of Canada.

Table of Contents

Executive Summary 3

Acknowledgement 4

Table of Contents 5

Introduction 8

Report Methodology 9

Focus Groups 9

Overview of the Scope of the Data Breach Problem 10

A Tale of Two Breaches 11

Epsilon 11

Figure 1: Canadian E-mail Notification of Epsilon Breach - Best Buy 12

Figure 2: Canadian E-mail Notification of Epsilon Breach - Air Miles 13

Sony Playstation 15

Defining Data Breaches 20

Legal Definition of Data Breach in Canada 21

Bill C-29/Bill C-12 Definition of Data Breach 23

Alberta PIPA Definition of Data Breach 24

Focus group participants' views of the definition of data breaches 24

Data Breach regulation in Canada Prior to Bills C-29/C-12 26

History of the OPCC Data Breach Guidelines since 2006 26

The OPCC Data Breach Guidelines 31

Bills C-29/C-12 32

Administrative Notification 32

Customer Notification 35

Focus Groups Participants Views of the Administrative and Customer Notification Thresholds 40

Alberta PIPA 43

Content of Notices 47

Administrative Notices 48

Alberta 49

Customer Notices 49

Under Bill C-12 49

Federally - Guidelines 51
Alberta 52
Timing of Notification 54
Administrative Notification 55
Under Bill C-12 55
Federally - Guidelines 55
Alberta 55
Customer Notification 56
Under Bill C-12 56
Federally - Guidelines 57
Alberta 57
Source of Notification (Responsibility to Notify) 59
Bill C-12 59
Under the Guidelines 62
Alberta 63
U.S. State Laws 64
Method of Notification 65
Encryption 68
Enforcement of Notification Duties 70
Bill C-12 70
Focus Groups Participants' Views of Enforcement Powers 74
Alberta 77
Enforcement for Breaches in Health Information Privacy 78
Private Right of Action 79
U.S. Data Breach Laws and New Developments 82
Data breach notification requirements under European Law 83
Statistics – How much breaching are Canadian organizations really doing? 85
Canadian Statistics 86
The TELUS-Rotman Joint Study on Canadian IT Security Practices 86
Office of the Privacy Commissioner of Canada 87
Alberta 88
British Columbia 88

Ontario 89
United States 89
Costs of a Data Breach 90
The Ponemon Institute's "The 2010 Annual Study: U.S. Cost of a Data Breach" Report 90
Stakeholder Interviews 93
Jacob Glick, Google 93
David Elder, Stikeman Elliott 94
David McMahon 95
Conclusion: A New Approach Needed 100
Recommendations 102
Appendix 1 - Focus Group Transcripts 104
Appendix 2 - Environics Report on Focus Groups 105
Appendix 3 - PIAC's notes on the Panel, entitled "Anatomy of a Data Breach" 106
Appendix 4 - PIAC Legal Memo on Data Breach Class Actions in Canada 110

Introduction

Data breaches are a modern consumer scourge. Born of large databases of personal information, these mishandlings of data by business, government or non-profit organizations appear to the Privacy Commissioner of Canada to be involving more records and becoming more serious by the month.[1] The potential results of data breaches for consumers are identity theft, serious disruption to banking and other commercial activities, mistrust of organizations, reluctance to engage in online commerce and general consumer disappointment and stress.

"Data breach" is a term that describes loss, unauthorized access to or unauthorized disclosure of individuals' personal information. Data breaches are thought popularly to describe mass losses, unauthorized accesses or disclosure, or at least those involving a number of individuals, rather than such incidents involving only one or a very few individuals. However, legal definitions tend to include breaches that can involve the records of even one single individual.

Organizations that deal with personal information can be roughly broken down into three categories for legal purposes in Canada: public sector (government) entities; private sector organizations (usually corporations such as retailers or consumer services providers);[2] and health care providers (doctors, hospitals and government or private sector actors dealing with personal health records). This report uses these rough categories (public sector; private sector; health) as the legislation and guidelines developed to deal with data breaches accept these categories.

This report seeks to examine the private sector data breach landscape to determine if the law and policy that is developing will help to protect consumers. Therefore this report focuses largely on consumers in general or customers of private sector organizations, with occasional references to health information data breach laws and practice (to date there are no public sector data breach notification laws).

Given the suspected magnitude and potential consumer harm from data breaches, PIAC undertook this research to attempt to assess whether the actual practice and proposed

[1] Sarah Schmidt, Postmedia News: " Privacy czar slams Sony for breach: Stoddart calls for power to levy 'significant, attention-getting' fines" (May 5, 2011). Online: http://www.ottawacitizen.com/story_print.html?id=4729207&sponsor= (accessed May 10, 2011).

[2] Certain private sector privacy laws require "commercial" activities be undertaken before an entity is subject to the law, for example, the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA"). Other acts have a different scope and therefore include the activities of charities, not-for-profit corporations and professional bodies such as regulatory colleges and unions. Quebec's *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1, for example, explicitly includes professional orders in s. 1.

legislation[3] was adequate to make a real difference for consumers and to identify the best approach to controlling data breaches in the private sector.

As will appear later, the answer appears to be that much can be done to improve Canada's data breach legislation and policy approach. Although the hour is late, there is still time to propose and effect these changes before the legal framework for data breaches in Canada is solidified federally.

Report Methodology

PIAC's methodological approach to this report was to gather primary research from four focus groups of Canadians regarding data breaches and interviews with key stakeholders and to augment that qualitative research with a secondary source literature review. PIAC undertook its own review of materials on data breaches kept in-house and tracked the progress of and interpreted proposed data breach legislation with its in-house and external counsel. This report builds upon PIAC's previous research on identity theft and electronic commerce.[4]

Focus Groups

In September 2010, PIAC conducted two focus groups of 6-8 individuals in Montreal and two of 6-8 individuals in Calgary. The two focus groups in Montreal were undertaken in French and the Calgary ones both in English. Transcripts and a focus group report prepared by the research firm Environics are appended to this report at Appendices 1 and 2, respectively.

As noted in the Environics report, PIAC sought both panels of focus group members that had been notified that their personal information had been breached and those that had not yet, to their knowledge, suffered this fate.[5]

---

[3] *An Act to amend the Personal Information Protection and Electronic Documents Act*, Bill C-12, 41st Parliament, 1st Session (2011). Online: http://www.parl.gc.ca/content/hoc/Bills/411/Government/C-12/C-12_1/C-12_1.PDF

[4] See Lawson and Lawford, " Identity Theft: The Need for Better Consumer Protection" (Ottawa, November 2003, PIAC). Online: http://www.piac.ca/files/idtheft.pdf. See also Lawford, " Identity Theft Insurance – Miserly Upon Misery" (Ottawa, November 2007, PIAC). Online: http://www.piac.ca/files/id_theft_insurance_misery_miserly.pdf.

[5] See Environics Report, Appendix 1, at p. 1:

> In support of this project, the PIAC engaged Environics Research Group to conduct qualitative research with two target populations, one consisting of Canadians who have experienced a loss or breach of their personal information and been notified of the loss or breach, and one consisting of Canadians who have never suffered such a loss (to their knowledge) and thus never been so notified. This research is designed to explore Canadians' reactions to a number of key

More information on the focus group methodology is found in the introductory pages of the Environics Report, found at Appendix 2.

Overview of the Scope of the Data Breach Problem

Canada at the federal level to date does not have a law requiring private sector organizations to report data breaches either to consumers or to the Privacy Commissioner of Canada, despite the fact that there is an overarching private sector privacy law. A bill to regulate the reporting of data breaches under the present private sector privacy legislation, PIPEDA,[6] was introduced in Parliament in 2010, died on the Order Paper and was reintroduced in the next Parliament in 2011.

The Office of the Privacy Commissioner of Canada has issued voluntary Guidelines for private sector organizations to consider if they wish to report the breach to her office or to consumers or customers. The OPCC reports on the number of voluntarily reported data breaches in her Annual Report each year. The latest Annual report shows this number is dropping.[7]

Currently four Canadian provinces have breach notification provisions in various privacy statutes. Ontario, New Brunswick and Newfoundland and Labrador have provisions in their privacy laws relating to health care, while Alberta has notification provisions in an Act that governs the protection of personal information in both the private and health sectors.

Each province's threshold for notification to individuals differs slightly. In Ontario's *Personal Health Information Protection Act* (PHIPA),[8] a health custodian is required to give notice to affected individuals any time health information about them is stolen, lost or accessed by unauthorized persons.[9] The New Brunswick *Personal Health Information Privacy and Access Act*

---

questions and assumptions in the ongoing debate over whether private and public sector actors should notify them if their personal data is lost, stolen or accessed by an unauthorized person, including such key issues as breach notification threshold (e.g., "risk"), timing, manner of notification, to whom notification is made, who should notify and remedies for a breach.

[6] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA").

[7] Office of the Privacy Commissioner of Canada, Annual Report to Parliament, 2010, Report on the Personal Information Protection and Electronic Documents Act (June 2011). Online: http://www.priv.gc.ca/information/ar/201011/2010_pipeda_e.pdf. See Section 4.8, page 85. The numbers of voluntarily reported data breaches are, respectively: 2008: 65; 2009: 58; 2010: 44.

[8] *Personal Health Information Protection Act 2004* , S.O. 2004 c. 3. s. 12 (2).

[9] Uniform Law Conference of Canada Civil Law Section Identify Theft Working Group Report 2010 *Uniform Protection of Privacy Act (Data Breach Notification)* Halifax, Nova Scotia August 2010 at p. 4. (ULCC 2010 Report).

(PHIPAA)[10] and Newfoundland and Labrador's *Personal Health Information Act* (PHIA)[11], require a custodian to notify an individual in breach situations if the breach will have an adverse effect on the provision of health care, or on the mental, physical, economic or social well-being of the individual. In Newfoundland and Labrador, the custodian must also notify the Commissioner of a material breach even in circumstances where it is not required by the Act.[12] Finally, consumers in Alberta now do, alone among Canadians, enjoy legal requirements on private sector organizations to report data breaches. The data breach provisions were added to Alberta's *Personal Information Protection Act* (PIPA) in 2009 and came into force May 1, 2010.[13] The privacy commissioner in Alberta, after receiving reports of breaches from organizations then determines if companies should report the breach to affected customers or clients.

A Tale of Two Breaches

Several recent high profile data breaches have surged into public view in the last year. These large breaches, while affecting many residents of the U.S., also affected thousands of Canadians. Although these breaches are only part of a much larger group, the study of which has provided interesting information on overall data breach trends,[14] we tell the tale of these two high profile breaches for their illustrative power and notoriety.

Epsilon

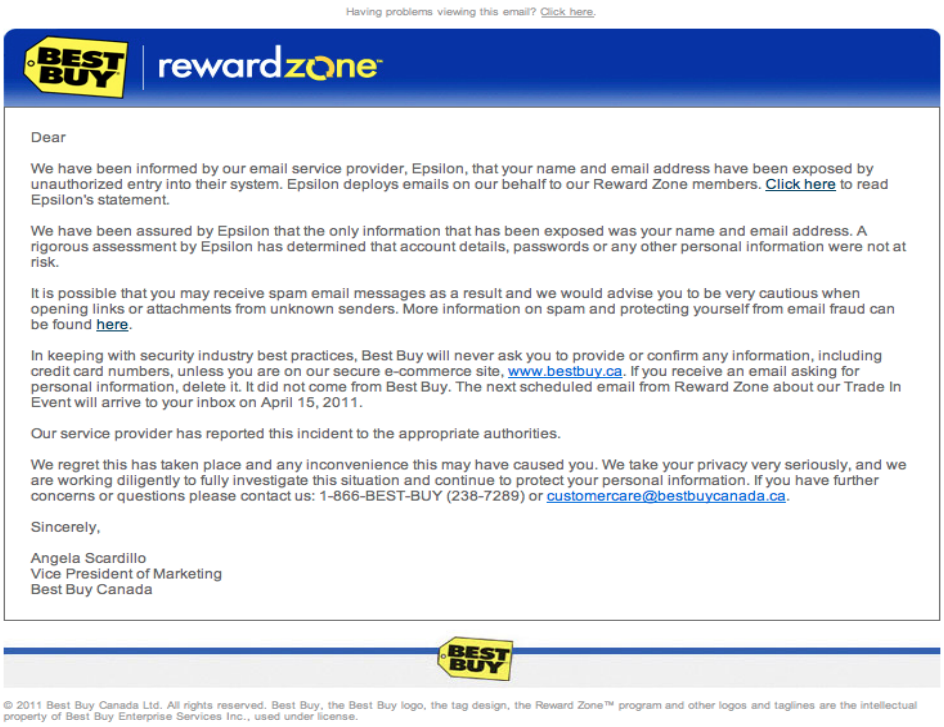
Epsilon is the world's largest permission-based email marketing provider. It sends more than 40 billion emails on behalf of 2,500 clients annually. On March 30, 2011, Epsilon discovered that millions of subscriber names and email addresses were compromised by hackers.[15] On April 1, 2011 Epsilon provided a brief warning of the breach to its corporate client base.[16] The release did not specify which clients were directly affected.[17] In turn, Epsilon's clients warned

[10] *Personal Health Information Privacy and Access Act* S.N.B. 2010 c. P-7.05 s. 49 (1) &(2). This act also has an additional exception in cases where the custodian reasonable believes that the breach will not lead to the identification the individual in question s. 49 (2) (c).
[11] *Personal Health Information Act* S.N.L. 2008 c. P-7.01 at s. 15 (3) – (8). [PHIA]
[12] PHIA s. at 15 (4).
[13] See *Personal Information Protection Act*, S.A. 2003, c. 6.5, section 34.1(1).
[14] See, *infra*, data security reports discussed in the section on Statistics, including the Verizon (2011) and TELUS-Rotman (2011) Reports.
[15] *Epsilon Notifies Clients of Unauthorized Entry into Email System* , online: Epsilon <http://www.epsilon.com/News%20&%20Events/Press%20Releases%202011/Epsilon_Notifies_Clients_of_Unauthorized_Entry_into_Email_System/p1057-l3>.
[16] *Epsilon Notifies Clients of Unauthorized Entry into Email System* , online: Epsilon <http://www.epsilon.com/News%20&%20Events/Press%20Releases%202011/Epsilon_Notifies_Clients_of_Unauthorized_Entry_into_Email_System/p1057-l3>.
[17] *Epsilon Breach Raises Specter of Spear Phishing*, online: KrebsonSecurity <krebsonsecurity.com/.../epsilon-breach-raises-specter-of-spear-phishing/>.

individual consumers of the privacy issue.[18] Public reports indicate at least 50 of the company's corporate clients were impacted,[19] meaning millions of private consumer information sets were stolen, including those of Canadians. See Figure 1 and Figure 2 on the next two pages for two example e-mail notices sent to Canadians in the wake of the Epsilon breach.

Figure 1: Canadian E-mail Notification of Epsilon Breach - Best Buy

From: "Best Buy Reward Zone" <rewardzone@email.bestbuyrewardzone.ca>
Date: April 3, 2011 10:20:29 PM MDT
To: _____
Subject: Important Email Security Alert



Having problems viewing this email? Click here.

BEST BUY | rewardzone

Dear

We have been informed by our email service provider, Epsilon, that your name and email address have been exposed by unauthorized entry into their system. Epsilon deploys emails on our behalf to our Reward Zone members. Click here to read Epsilon's statement.

We have been assured by Epsilon that the only information that has been exposed was your name and email address. A rigorous assessment by Epsilon has determined that account details, passwords or any other personal information were not at risk.

It is possible that you may receive spam email messages as a result and we would advise you to be very cautious when opening links or attachments from unknown senders. More information on spam and protecting yourself from email fraud can be found here.

In keeping with security industry best practices, Best Buy will never ask you to provide or confirm any information, including credit card numbers, unless you are on our secure e-commerce site, www.bestbuy.ca. If you receive an email asking for personal information, delete it. It did not come from Best Buy. The next scheduled email from Reward Zone about our Trade In Event will arrive to your inbox on April 15, 2011.

Our service provider has reported this incident to the appropriate authorities.

We regret this has taken place and any inconvenience this may have caused you. We take your privacy very seriously, and we are working diligently to fully investigate this situation and continue to protect your personal information. If you have further concerns or questions please contact us: 1-866-BEST-BUY (238-7289) or customercare@bestbuycanada.ca.

Sincerely,

Angela Scardillo
Vice President of Marketing
Best Buy Canada

BEST BUY

Partner company Return Path – which provides monitoring and authentication services to email providers - warned Epsilon of a possible data breach on November 24, 2010. Return Path communicated that companies like Epsilon were under an "an organized, deliberate, and destructive attack clearly intent on gaining access to industry-grade email deployment systems."[20] Specifically, Epsilon was told that the phishing attacks were targeted only at staff responsible for email operations at more than 100 different service providers.

[18] *Epsilon Breach Raises Specter of Spear Phishing*, online: KrebsonSecurity <krebsonsecurity.com/.../epsilon-breach-raises-specter-of-spear-phishing/>.
[19] Big Hack Attack: Writing Was on the Wall: online: CBS News <http://www.cbsnews.com/stories/2011/04/07/tech/cnettechnews/main20051895.shtml>.
[20] Spear Phishing Attacks Snag E-Mail Marketers, online: Krebs on Security <http://krebsonsecurity.com/tag/return-path/>.

Epsilon became aware that such spear phishing attacks could be successful when client Walgreens fell victim to a data breach on December 10 (Walgreens promptly filed a request that Epsilon increase security measures against spear phishing at this time). The message was furthered three days later when fellow email service provider Silverpop was affected by a similar attack.

Figure 2: Canadian E-mail Notification of Epsilon Breach - Air Miles

From: AIR MILES Reward Program <newsandmore@emails.airmiles.ca>
Date: April 4, 2011 8:22:24 PM MDT
To:
Subject: An important email security update for AIR MILES Collectors
Reply-To: "newsandmore" <1fb04a007layfovciawsokyyaaaaabradjzxsi5gohayaaaaa@emails.airmiles.ca>

Can't view this email? Click here to view it online.

The AIR MILES® Reward Program was informed by our email service provider that they had an unauthorized entry into their email platform, which is the system used to send AIR MILES emails. We have been assured that the only information that may have been exposed was first name, last name and email address of some of our Collectors. Details of your account are not stored in this system and were not at risk.

Please note it is possible you may receive spam email messages as a result. We want you to be cautious when opening links or attachments from unknown third parties. We want to remind you that AIR MILES will never ask for your personal information or login credentials in an email. As always, be cautious if you receive emails asking for your personal information and be on the lookout for unwanted spam. It is not our practice to request personal information by email.

As a reminder, we recommend that you:
- Don't give your AIR MILES Collector number or PIN in email.
- Don't respond to emails that require you to enter personal information directly into the email.
- Don't respond to emails threatening to close your account if you do not take the immediate action of providing personal information.
- Don't reply to emails asking you to send personal information.

We regret that this has taken place and apologize if this causes you any inconvenience. We take your privacy very seriously and we will continue to work diligently to protect your personal information.

If you have any questions please contact us at question@airmiles.ca or 1-888-AIR MILES.

airmiles.ca | Update your email | Contact Us | Privacy | Legal | airmilesshops.ca | unsubscribe

Please do not reply to this email.
If you have any questions or comments, contact us.

®™ Trademarks of AIR MILES International Trading B.V. Used under license by LoyaltyOne, Inc. Sponsor, Supplier and Retailer trademarks are owned by the respective Sponsors, Suppliers or Retailers or authorized for their use in Canada.

In response, Epsilon initiated the design of an alert program created to flag unusual data download patterns. However, it did not notify its clients of phishing attacks at the time. The

alert program eventually launched on March 30, discovering a breach that affected millions of consumers.[21]

Epsilon issued a brief statement in response on April 1, 2011.[22] There, the service provider identified that a subset of clients had been affected. While Epsilon refused to provide a specific list of clients involved, that very list was developed by privacy blogger Brian Krebs three days later. He indentified heavy-hitters like JD Morgan Chase, Citibank, US Bank, Barclay's Bank, Capital One and TD Ameritrade as some of the largest corporations impacted.[23]

The breach provided email addresses and full names of consumers to the criminals responsible. It is known that acquiring this information is the first hurdle which hackers must clear before they can gain even more valuable information from targeted individuals. After acquiring such name and e-mail information, hackers are able to personalize emails to specific users, posing as a company that the user is comfortable with in an effort to exploit them. For example, if a user's records indicate he or she is a client of Citibank, hackers could then send a personalized email with a forged Citibank facade, attempting to coerce the user to provide confidential information (passwords or credit card numbers), which the hackers may exploit for financial gain. Two to three percent of the population likely will fall victim to phishing emails.[24] Here, passwords may be provided, credit card numbers attained, or programs downloaded to allow for malware installation. These damaging efforts could not occur but for a hacker's knowledge of the targeted user's name, email address, and established business relationships. Thus, it may be seen that the Epsilon breach had and continues to have serious potential consequences for individual consumers.

When asked about the Epsilon breach, Jonathan Zittrain, a professor at Harvard Law School and co-founder of the Berkman Center for Internet & Society remarked: "the right security controls – or overall architecture, not keeping a Ft. Knox of email addresses lazily on the Internet, even behind a password – could prevent this."[25] Such a sentiment has been echoed by information

[21] The Epsilon data breach affected millions – so what happens next?, online: The Tech Herald <http://www.thetechherald.com/article.php/201114/7011/The-Epsilon-data-breach-affected-millions-so-what-happens-next>.
[22] Epsilon Notifies Clients of Unauthorized Entry into Email System , online: Epsilon <http://www.epsilon.com/News%20&%20Events/Press%20Releases%202011/Epsilon_Notifies_Clients_of_Unauthorized_Entry_into_Email_System/p1057-l3>.
[23] Epsilon Breach Raises Specter of Spear Phishing, online: KrebsonSecurity <krebsonsecurity.com/.../epsilon-breach-raises-specter-of-spear-phishing/>.
[24] Canadian consumers among victims of massive email security breach, online: The Vancouver Sun <http://www.vancouversun.com/news/Canadian+consumers+among+victims+massive+email+security+breach/4558021/story.html>.
[25] Thousands more Canadians notified of email hacking, online: Toronto Star <http://www.thestar.com/business/article/969130--thousands-more-canadians-notified-of-email-hacking>.

security specialists, who advocate for encryption to occur at both the network and storage levels.

It should be noted that those who opted-out of affected email lists were also impacted by the data breach. This means that people who had specifically asked Epsilon to remove them from their data lists were made vulnerable to phishing attacks. Additionally, it has been argued that the quality of the list attained will allow for long-term exploitation which could occur in six or 12 months, a time when most have forgotten about the incident itself, and are thus more vulnerable to phishing efforts.

Since the breach, Epsilon has continued to investigate the incident and is cooperating with law enforcement in an effort to apprehend those responsible. The company has invested in additional resources to monitor unusual or suspicious activity, and has engaged third party services to review and recommend additional hardening of the company's security controls.[26]

Sony Playstation

Sony's PlayStation Network is an online portal that allows for socializing and commercial activity related to video games, music, and film. The network was breached by hackers for a three-day period, which began April 17, 2011.[27] The data breach has been classified as unprecedented,[28] mammoth,[29] and as one of the five largest ever seen.[30] It affected more than one million Canadians,[31] and over 77 million PlayStation users in total.[32] The criminals responsible gained access to PlayStation user names, birthdays, home addresses, email addresses, network passwords, network logins, purchase histories, and billing addresses.[33] PlayStation initially specified that there was no evidence that credit card data was taken;[34]

---

[26] Epsilon Response to House Committee on Energy and Commerce, online: House Energy and Commerce Committee <http://republicans.energycommerce.house.gov/Media/file/Letters/041811%20Epsilon%20Response.pdf>.
[27] Direct Targeting: PlayStation breach proves attackers seek large databases, online: Info Executive <http://infoexecutive.itincanada.ca/index.php?id=14145&cid=78 >.
[28] Sony offers PlayStation network users $1M insurance after hacking, online: The Seattle Times <http://seattletimes.nwsource.com/html/businesstechnology/2014985875_sonysorry07.html>.
[29] Analyst: PlayStation Network Fiasco Will Be Costly, Change Industry Forever, online: Time Techland <http://techland.time.com/2011/04/27/analyst-playstation-network-fiasco-will-be-costly-change-industry-forever/#ixzz1M4Loy7Jp>.
[30] PlayStation data breach deemed in 'top 5 ever', online: CBC News <http://www.cbc.ca/news/business/story/2011/04/27/technology-playstation-data-breach.html>.
[31] PlayStation data breach deemed in 'top 5 ever', online: CBC News <http://www.cbc.ca/news/business/story/2011/04/27/technology-playstation-data-breach.html>.
[32] Direct Targeting: PlayStation breach proves attackers seek large databases, online: Info Executive <http://infoexecutive.itincanada.ca/index.php?id=14145&cid=78 >.
[33] Update on PlayStation Network and Qriocity, online: PlayStation Blog <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>.
[34] Update on PlayStation Network and Qriocity, online: PlayStation Blog <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>.

however, the company later admitted that the encrypted credit card numbers of 10 million users might have been attained.[35]

PlayStation learned its servers were compromised on April 19, but was not aware of the extent of the breach.[36] A shutdown of the PlayStation network was undertaken at this time. The company mobilized an internal inspection team on April 20, and augmented that group over the following two days.[37] On April 23, it was found that a highly sophisticated intruder gained unauthorized access to the servers and hid its presence from system administrators.[38] By April 25, the forensic teams confirmed the scope of personal data believed to have been breached, but were unsure about credit card information access. Public notice of the breach was given on April 26.[39] Admission of the vulnerable credit cards did not arrive until May 1,[40] when the company stated, "we cannot rule out the possibility [that credit card information was breached]."[41]

In a letter addressed to U.S. Senator Richard Blumenthal, Sony explained that conflicting U.S statutes, combined with the international scale of the issue made disclosure difficult, stating: "there are a variety of state statutes that apply, and several that have conflicting or inconsistent requirements, but given the global nature of the network, SNEA [Sony Network Entertainment America] needed to be mindful of them all - and has endeavored to comply with them all".[42] Additionally, Sony explained that it "was very concerned that announcing incomplete, tentative

[35] Sony Considers Reimbursing Credit Card Replacement Costs In Light Of Data Breach, online: Kotaku http://www.kotaku.com.au/2011/05/sony-considers-reimbursing-credit-card-replacement-costs-in-light-of-data-breach/

[36] Blumenthal on Sony Response: "A Strong First Step", online: Richard Blumenthal United States Senator for Connecticut <http://blumenthal.senate.gov/press/release/index.cfm?id=E347AED3-DF21-493D-BAA6-BAFA9FF12F84>.

[37] Blumenthal on Sony Response: "A Strong First Step", online: Richard Blumenthal United States Senator for Connecticut <http://blumenthal.senate.gov/press/release/index.cfm?id=E347AED3-DF21-493D-BAA6-BAFA9FF12F84>.

[38] Blumenthal on Sony Response: "A Strong First Step", online: Richard Blumenthal United States Senator for Connecticut <http://blumenthal.senate.gov/press/release/index.cfm?id=E347AED3-DF21-493D-BAA6-BAFA9FF12F84>.

[39] Sony says planted file in attack was named 'Anonymous', online: CNET News <http://news.cnet.com/8301-27080_3-20059737-245.html>.

[40] Sorry Sony admits it held 10m credit card, online: ITNews <http://www.itnews.com.au/News/256007,sorry-sony-admits-it-held-10m-credit-cards.aspx>.

[41] Update on PlayStation Network and Qriocity, online: PlayStation Blog <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/>.

[42] Blumenthal on Sony Response: "A Strong First Step", online: Richard Blumenthal United States Senator for Connecticut <http://blumenthal.senate.gov/press/release/index.cfm?id=E347AED3-DF21-493D-BAA6-BAFA9FF12F84>.

or potentially misleading information to consumers could cause confusion and lead them to take unnecessary actions."[43]

A second Sony breach (which actually pre-dated the initially reported breach) was discovered on May 2, adding another 24.6 million impacted users and 20,000 credit card and bank account numbers to the already prodigious amount of stolen private information.[44]

A third breach was discovered on May 7 when independent Japanese security researchers searched Sony's public servers.[45] The researchers found the names and partial addresses of 2,500 sweepstakes contestants on a server readable by anyone.[46] Two days after its discovery, Sony announced that the file was removed from public access.[47]

The wealth of information that hackers have attained leaves individual PlayStation consumers vulnerable. Phishing attacks are probable, and infected units may provide further personal and financial information to hackers, or may be exploited to create a botnet to power another large-scale attack.

Harsh criticism has followed the PlayStation breaches. The spotlight has been especially bright as the Japanese company's debacle arrived closely after the data breach of American email marketing provider Epsilon. These attacks affirmed that criminal hackers are most interested in attacking large data stores.[48] This follows a 2009 trend, where 96% of record breaches came from servers.[49]

As the PlayStation and Epsilon systems were unregulated, debate now revolves around a need for regulatory standards set to protect large databases of personal information. At present, encryption providers criticize a perceived industry hesitation to protect large data stores.[50]

---

[43] Blumenthal on Sony Response: "A Strong First Step", online: Richard Blumenthal United States Senator for Connecticut <http://blumenthal.senate.gov/press/release/index.cfm?id=E347AED3-DF21-493D-BAA6-BAFA9FF12F84>.

[44] Sony's CEO under fire as 25 million more accounts hacked, onilne: The Vancouver Sun <http://www.vancouversun.com/Sony+under+fire+million+more+accounts+hacked/4718203/story.html#ixzz1M4PYcv73>

[45] Sony delays PSN restart as third breach is discovered, online: SC Magazine <http://www.scmagazineus.com/sony-delays-psn-restart-as-third-breach-is-discovered/article/202465/>.

[46] Sony delays PSN restart as third breach is discovered, online: SC Magazine <http://www.scmagazineus.com/sony-delays-psn-restart-as-third-breach-is-discovered/article/202465/>.

[47] Sony removes data posted by hackers, delays PlayStation restart, online: Reuters <http://www.reuters.com/article/2011/05/07/sony-idUSL3E7G701T20110507>.

[48] Direct Targeting: PlayStation breach proves attackers seek large databases, online: Info Executive <http://infoexecutive.itincanada.ca/index.php?id=14145&cid=78 >.

[49] Direct Targeting: PlayStation breach proves attackers seek large databases, online: Info Executive <http://infoexecutive.itincanada.ca/index.php?id=14145&cid=78 >.

[50] Direct Targeting: PlayStation breach proves attackers seek large databases, online: Info Executive <http://infoexecutive.itincanada.ca/index.php?id=14145&cid=78 >.

They advocate that protecting information is not only more just, but it is also more cost-effective than leaving private data vulnerable to attack.

The effect of the breach has not only impacted Sony customers, but also the company itself. PlayStation's stock fell more than eight percent 48 hours after the breach was announced.[51] Questions about the corporation's leadership quickly arose.[52] The revenue-generating PlayStation Network was forced to shut down on April 20, with a re-launch goal of set for the end of May.[53] Many estimate that the breach will cost between 1.5 and 2 billion dollars to correct, including loss of business and the cost of cleansing the PlayStation Network.[54] However, Forbes has held the cost could be as high as $24 billion, citing a study from security think tank Ponemon that pins a data breach's cost at up to $318 per person affected.[55]

The Sony breach also may destabilize insurance rates for companies holding large stores of personal information, as companies facing breach notification and other costs look to their insurers for indemnification. In the Sony case, the insurance claim is likely to be in excess of $ 2 billion.[56] Sony has already indicated it will be seeking insurance payouts under its corporate insurance policies.[57]

In response to the debacle, Sony warned its customers to change their passwords and usernames, advised them not to share personal information online, and promised to not ask for personal information itself. It also created the position of Chief Information Officer of Sony Corporation.

The company has also offered affected users in the U.S. a free 12-month subscription to a cyber monitoring and surveillance program called AllClear ID Plus.[58] Provided by Debix Inc;[59] the

[51]PlayStation Network hack causes drop in Sony share prices, online: PlayStation Universe <http://www.psu.com/PlayStation-Network-hack-causes-drop-in-Sony-share-prices--a011485-p0.php>.
[52] Sony CEO under fire as 25 million more accounts hacked, online: Ottawa Citizen <http://www.ottawacitizen.com/Sony+under+fire+million+more+accounts+hacked/4718203/story.html>.
[53] Sony PlayStation Network may not be back online before May 3, online: Metro UK 1<http://www.metro.co.uk/tech/games/862731-sony-playstation-network-may-not-be-back-online-before-may-31>.
[54] PlayStation Network hack could cost Sony 1.5 Billion, online: Metro UK http://www.metro.co.uk/tech/games/861936-playstation-network-hack-could-cost-sony-1-5billion.
[55] Sony: Credit risked in PlayStation outrage, online: Forbes <http://www.forbes.com/feeds/ap/2011/04/26/technology-specialized-consumer-services-us-sony-playstation-credit-cards-warning_8436469.html>.
[56] Sony Data Breach Raises Insurance Issues, online: Miller Thompson Lawyers <http://millerthomson.com/en/blog/ontario-insurance-litigation-blog/sony-data-breach-raises-insurance-issues>.
[57] Sony Data Breach Raises Insurance Issues, online: Miller Thompson Lawyers <http://millerthomson.com/en/blog/ontario-insurance-litigation-blog/sony-data-breach-raises-insurance-issues>.
[58] Although Sony announced that: "We are working to make similar programs available in other countries/territories where applicable. Information will be posted on local websites/blogs when available" on May

program monitors the internet to detect exposure of any AllClear ID Plus customer's personal data. It also provides monthly status reports and prompt alerts if the misuse of personal information is found (alerts are said to include where and when a fraudulent act has occurred). Further, if privacy issues are detected, Sony claims users will have access to an on-call licensed private investigator who will undertake a comprehensive inquiry on the user's behalf. If identity theft occurs, a restoration specialist will also be made available.[60]

Additionally, the AllClear ID plan provides a $1-million identity theft insurance policy to affected clients. According to PlayStation, the insurance policy will "provide financial relief of up to $1 million for covered identity restoration costs, legal defense expenses, and lost wages that occur within 12 months after the stolen identity event."[61]

A class action suit on behalf of PlayStation Network and Qriocity (the music and movie arm of the PlayStation Network) users was launched on May 4 in Ontario. There, one billion dollars are being sought to cover costs of credit card monitoring and fraud insurance for two years. The claim alleges Sony exposed its users to identity theft, theft from bank and credit cards, and "fear, anxiety (and) emotional distress."[62] A similar action was begun in Massachusetts on behalf of American customers.[63]

Sony's data breach was not reported to Canada's Privacy Commissioner despite the 2007 voluntary guidelines on data breaches. In the wake of the breach, the Commissioner stated, "I remain deeply troubled by the large number of major breaches we are seeing. Too many companies are collecting more personal information than they are able to effectively protect."[64] The Commissioner then called for power to impose "attention-getting" fines for similar data breaches, stating, "the only way to get some corporations to pay adequate

---

5, 2011, (see: http://blog.us.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/) no such program in Canada has yet been offered.

[59] Sony Offering Free 'AllClear ID Plus' Identity Theft Protection in the United States through Debix, Inc., online: PlayStation Blog <http://blog.us.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/>.

[60] Sony Offering Free 'AllClear ID Plus' Identity Theft Protection in the United States through Debix, Inc., online: PlayStation Blog <http://blog.us.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/>.

[61] Sony Offering Free 'AllClear ID Plus' Identity Theft Protection in the United States through Debix, Inc., online: PlayStation Blog <http://blog.us.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/>.

[62] Ontario woman suing Sony over PlayStation breach, online: The Globe and Mail <http://m.theglobeandmail.com/news/national/ontario/ontario-woman-suing-sony-over-playstation-breach/article2008792/?service=mobile>.

[63] Mass. Woman among 1st to sue Sony over data breach, online:Boston Business Journal <http://www.bizjournals.com/boston/news/2011/05/06/mass-woman-among-1st-to-sue-sony.html>.

[64] Canada's privacy commissioner wants heft fines for data breaches¸online: The Globe and Mail <http://m.theglobeandmail.com/news/technology/tech-news/canadas-privacy-commissioner-wants-hefty-fines-for-data-breaches/article2009801/?service=mobile>.

attention to their privacy obligations is by introducing the potential for large fines that would serve as an incentive for compliance."[65]

The Commissioner's comments arrive at a time that is seeing more private information gathered by corporations with less protection for consumers often following. For example, major issues have arisen with the gaining popularity of cloud-based technology, data management solutions that permit for remote access to data that is physically stored elsewhere.[66] Dartmouth university professor Eric Johnson has said that the combination of cloud technology and private information means, "[n]obody is secure."[67]

The PlayStation breaches were very serious in nature, and part of a dangerous trend. In total, the private information of over 100 million consumers was stolen in one fell swoop. A tentative preliminary price tag of 2 billion dollars (U.S.) has been estimated as necessary for mitigation. Consumer confidence has been justifiably shaken. Now, Sony recognizes that "cybercriminals will continue to attack businesses, consumers, and governments, posing a real threat to our economy and security," and that "a strong coalition among government, industry, and consumers is needed to identify ways that the public and private sectors can work more closely together to enact strong laws, promote stronger enforcement of those laws, educate people about the threats we face, share best practices and make the Internet a safe place for everyone to engage in commerce."[68]

Defining Data Breaches

The definition of "data breach" is evolving, however, it has generally been accepted by lawmakers and policymakers to be a term that describes loss, unauthorized access to or unauthorized disclosure of one, several or many individuals' personal information. Such loss or interference with the data can be the result of many factors, but ranges from: simple loss of a USB key or laptop or theft of these physical devices (or even hard drives or whole servers); unauthorized remote system entry (hacking); and employee or contractor access beyond that

[65]" Canada's privacy commissioner wants hefty fines for data breaches"¸ *supra*, at fn 1.
[66] Reaching for the Cloud(s): Privacy Issues related to Cloud Computing, online: Office of the Privacy Commissioner of Canada < http://www.priv.gc.ca/information/pub/cc_201003_e.cfm>.
[67] Sony data breach may rain on cloud computing, online: Shanghai Daily <http://www.shanghaidaily.com/nsp/Business/2011/05/09/Sony%2Bdata%2Bbreach%2Bmay%2Brain%2Bon%2Bcloud%2Bcomputing/>. Note however, *infra*, the comments of Jacob Glick, Canada Policy Counsel for Google, who argues that cloud computing actually reduces the risk of ID theft as cloud computing is more secure than many portable media devices.
[68] Blumenthal on Sony Response: "A Strong First Step", online: Richard Blumenthal United States Senator for Connecticut <http://blumenthal.senate.gov/press/release/index.cfm?id=E347AED3-DF21-493D-BAA6-BAFA9FF12F84>.

required for the job, especially for malicious or unauthorized purposes. In addition, data breaches can also be unrelated to computer technology, as when paper employment or patient records are disposed of in open trash containers without being shredded. However, the majority of the largest breaches involve considerable electronic records and computer access. Therefore this report will concentrate more on data security and data breaches in the electronic realm than the physical realm.

Legal Definition of Data Breach in Canada

Most legislation in force in the United States, Canada and many other countries approximates the definition created for the first data breach law, California's S.B. 1386, first in force in 2002. That statute describes both "personal information" (which is a narrowly defined list of particular information items, unlike Canada's definition in federal privacy legislation) and "breach of the security of the system". The breach element is thus defined in terms of the system that created it. California's law requires that the information be "computerized data" thus the covered data breaches are only of computerized data held in a computer system, not hard copy files. The actual breach is defined as a breach of security of the computer system allowing access to the personal information:

> "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.[69]

Legislation recently that has been introduced in Canada to require reporting of data breaches (discussed below) includes a definition of “security breach” which is intended to cover the field that was defined above regarding data breaches and other security failures. Prior to this time, however, there was a definition of data breach developed in Canada by the Office of the Privacy Commissioner of Canada in consultations with industry and some consumer groups in 2006. It read thus: "A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information. Such activity is “unauthorized” if it occurs in contravention of applicable privacy legislation, such as PIPEDA, or similar provincial privacy legislation."[70]

---

[69] California Civil Code, §1798.29(d). See also, for example, Illinois *Personal Information Protection Act*, 815 Ill. Comp. Stat. 530/.

[70] Privacy Commissioner of Canada Guideline: "Key Steps for Organizations in Responding to Privacy Breaches" (Ottawa: 2007, Office of the Privacy Commissioner of Canada), at p. 1. ("Guidelines" or "Key Steps"). Online: http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf (accessed May 10, 2011).

Interestingly, the Guideline definition covered unauthorized "use", which would cover accesses to, or unauthorized modifications of, personal information internal to an organization.

Bill C-29 / Bill C-12 Definition of Data Breach

Bill C-29, *An Act to amend the Personal Information Protection and Electronic Documents Act*, with the short title "Safeguarding Canadians' Personal Information Act," died on the order paper on the dissolution of the 40th Parliament in late March 2011. The Bill was reintroduced in effectively identical form in the 41st Parliament in October 2011 as Bill C-12 (with the same title) when the Conservative government received a majority in the federal 2011 election.[71]

This Bill provides amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) that are designed to: "require organizations to report material breaches of security safeguards to the Privacy Commissioner and to notify certain individuals and organizations of breaches that create a real risk of significant harm."[72] The Bill tackles the definitional question of a "data breach" by defining a "breach of security safeguards" which means: "the loss of, unauthorized access to, or unauthorized disclosure of, personal information resulting from a breach of an organization's security safeguards that are referred to in clauses 4.7 to 4.7.5 of Schedule 1 or from a failure to establish those safeguards."[73] The Bill thus covers loss of data, unauthorized access to data and unauthorized disclosure of data. Presumably, an access in good faith by an employee within an organization for the purposes only of the organization and which did not lead to further disclosures would not fall afoul of this definition, but it is not spelled out, as in the California legislation. It would perhaps require a finding by the Office of the Privacy Commissioner of Canada to this effect.

Referring explicitly to the general security requirements of PIPEDA, the bill also defines a "failure to establish" security safeguards to be a breach. This is because PIPEDA requires organizations to protect personal information "by security safeguards appropriate to the sensitivity of the information."[74] Interestingly, in PIPEDA Principle 4.7.1, the definition of "security safeguards" in that Principle is wider than that in the Bill, in that unauthorized "copying", "use" and "modification" of personal information are also to be prevented with adequate security safeguards. Arguably, since the Bill's definition incorporates the security

[71] See Library of Parliament, Legislative Summary of Bill C-12, An Act to Amend the Personal Information Protection and Electronic Documents Act (Ottawa: Publication Number 41-1-C12-E, 19 October 2011) at p. 1: "It is a reintroduction of Bill C-29, which died on the Order Paper following the dissolution of the 40th Parliament on 26 March 2011." Online: http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/1/c12-e.pdf

[72] See Bill C-29, An Act to Amend the Personal Information Protection and Electronic Documents Act, "Summary", at para. (i). Online: http://www.parl.gc.ca/content/hoc/Bills/403/Government/C-29/C-29_1/C-29_1.PDF. Bill C-12 has the identical note.

[73] Bill C-29/C-12, at cl. 2(3) "Breach of Security Safeguards".

[74] PIPEDA, Principle 4.7.

safeguards from PIPEDA, the unauthorized "copying", "use" and "modification" of personal information could qualify as a "breach of security safeguards". However, to remove doubt, it would perhaps have been preferable to include "copying", "use" and "modification" of personal information as *per se* breaches of security.[75]

Alberta PIPA Definition of Data Breach

Alberta does not take the approach of defining a "breach of security safeguards" but rather posits a duty on organizations to "protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction."[76] The Alberta *Personal Information and Protection Act* (PIPA) approach of requiring "reasonable security arrangements" is coupled with a concomitant duty in s. 34.1 to report a breach that would create a "real risk of significant harm to an individual".

Focus group participants' views of the definition of data breaches

Focus group participants were led in discussion by a moderator who first asked participants what they thought was meant by the term "data breach" unprompted, then introduced the concept of data breaches by reading the definition of "security breach" from Bill C-29. In all of the groups, the participants stressed that unauthorized access, as well as disclosure, could be considered a data breach, some before hearing the "official" definition from the Bill. For example, the first Calgary group offered these ideas before hearing the definition:

> Moderator
>
> M. "[. . .] what does it mean to you when you hear “data breach”?"
>
> Respondent 1 (Calgary)
>
> R. Somebody’s gotten into a piece of data that should be secured, but it’s not and it’s open publicly or it’s something that should be secured and it’s not.
>
> Respondent 2 (Calgary)

[75] Due to these extra steps, it seems prudent to put more into the initial definition of a security breach from the PIPEDA security safeguards. One can imagine a mass hacking incident where personal details were modified on many financial accounts, such as changing logins or passwords to all be the same, which might not otherwise qualify as a "breach of security safeguards" on Bill C-29/C-12's definition but would almost certainly otherwise require reporting and likely also notification to individuals due to the likelihood of financial harm.
[76] PIPA, s. 34.

R. Any one of a number of ways. Basically somebody has accessed data that they really shouldn't have accessed, whether or not they forced their way in or not.[77]

These participants clearly included internal inappropriate accesses within the scope of a data breach (unprompted) and further, mentioned the idea that a failure to properly secure data could be tantamount to an actual breach with a public disclosure. This result was surprising, in that the research script developed by PIAC and Environics had assumed most participants would have conceived their ideas about data breaches from press reports of actual public disclosures of personal information, which tend to involve fact situations where data has been accessed or disclosed outside of an organization. The concept that corporations and other organizations had a responsibility to have adequate security was strongly expressed both unprompted and even more strongly after a definition including security was read.

A particular example comes from the same Calgary group as a respondent describes a high school data breach:

M: Now, have any of you heard of any data breaches recently in the news? Like have there been any that have gotten any publicity or anything?

R1: I haven't heard of anything major with our district, but obviously there are a lot of smart students that are very good at computers and they're constantly trying to get into our database to … well, they've gone in there to change marks.

M: Oh, really?

R2: Pretty clever kids.

R1: So I've heard about two or three students that have done that in the last couple of years.

M: But has it ever been a data breach that involved like, I don't know, getting the personal information?

R1: Yeah. Well, once they get in there they can access anybody's file and they can access anybody's marks. So yeah, they can get lots of information.[78]

Focus group participants appeared to firmly accept the concept that unauthorized access to personal data qualified as a "data breach" and that the particular instances of data breaches implicated the "security safeguards" of the organization or institution involved.

[77] Calgary Focus Group 1 at p. 4.
[78] Calgary Focus Group 1 at pp. 4-5.

The definition of "data breach" settled on in Bill C-29/C-12 therefore appears to adequately reflect the expectations of an organization's customers as that the framework for regulating data under PIPEDA, especially as it references PIPEDA's Safeguards principle.

Data Breach regulation in Canada Prior to Bills C-29/C-12

History of the OPCC Data Breach Guidelines since 2006

The Office of the Privacy Commissioner reacted to initial pressure to deal with data breaches over 6 years ago by creating voluntary breach notification guidelines, which are still in use by organizations today.[79] Before outlining these present voluntary rules, it is crucial to understand the history of efforts to introduce mandatory breach notification in legislation, which helps to explain in part why Canada has, and continues to have, only voluntary disclosures under non-binding guidelines as well as why Bill C-29/C-12 were/are structured as they were/are.

These guidelines were the product of a stakeholder consultation held in April 1997 and anticipated the Industry Committee's report after the statutory review of the *Personal Information Protection and Electronic Documents Act*.[80] In that review, the Privacy Commissioner asked that the government consider introducing breach notification legislation as part of PIPEDA in two separate appearances. However, in her first appearance on the PIPEDA review,[81] the Privacy Commissioner stated she needed more information on data breach notification and whether, for example, it led to identity theft. However, before her

[79] The four guideline documents are found on the Privacy Commissioner's webpage at: http://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_e.cfm The main (and original) undated document is entitled "Key Steps for Organizations in Responding to Privacy Breaches". See online: http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf

[80] In an unpublished letter to the OPCC dated April 19, 2007, PIAC was highly critical of the OPCC's parallel process on data breach consultations. PIAC argued the OPCC should wait for the ETHI committee report before drafting data breach notification guidelines. PIAC also objected to the drafting of the OPCC draft guidelines: "In particular, the fact that the drafting of the document was left to two lawyers from Canada's two largest telephone companies, which have an obvious interest in minimizing disclosure of data breaches, is unacceptable. At the least the OPCC staff should have developed the draft and, if input was solicited on the draft, that input should come from all stakeholders. We instead were presented with a *fait accompli*, and our objections to the fundamental scope and direction of the document therefore appeared to be unreasonable. This is not so and would have been greatly helped by a more impartial drafting process."

[81] The transcript of the Privacy Commissioner's first appearance before the ETHI Committee is found in the: 39th PARLIAMENT, 1st SESSION, Standing Committee on Access to Information, Privacy and Ethics, Monday, November 27, 2006. Online: http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2544266&Language=E&Mode=1

second appearance at the PIPEDA review in February 2007,[82] there had been high profile data breaches in the U.S. (also involving Canadians) and Canada. These developments appeared to steel the Privacy Commissioner's resolve to call for a limited breach notification requirement in PIPEDA.[83] Her call was limited, however, by her reticence to ask for any order-making power to buttress the new requirement,[84] her lack of specific potential wording for the Committee[85] and her faith in the voluntary guidelines her Office was then in the process of developing.[86]

The Industry Committee nonetheless reacted to other witnesses calling for more stringent mandatory data breach notification rules[87] and recommended "that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner" and that the Privacy Commissioner then have the discretion whether to require companies or organizations to notify individuals. Finally, the Committee recommended that "in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud."[88]

While the ETHI committee was preparing its report, the OPCC was preparing its draft guidelines.

The saga of the data breach guidelines and the notification amendments to PIPEDA was not over, however, as Industry Canada, in an unusually vigorous departmental reaction to the Industry Committee's report, issued its own report which argued for a very high threshold for

---

[82] The transcript of the Privacy Commissioner's second appearance before the ETHI Committee is found in the: 39th PARLIAMENT, 1st SESSION, Standing Committee on Access to Information, Privacy and Ethics, Thursday, February 22, 2007. Online: http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2735086&Language=E&Mode=1&Parl=39&Ses=1 (OPCC Second ETHI Appearance).

[83] See OPCC, Annual Report to Parliament 2006 - Report on the Personal Information Protection and Electronic Documents Act, a p. 2: "A separate set of media reports about major data breaches also provoked concern by Canadians toward the end of 2006. A few private sector organizations – notably a mutual fund subsidiary of the Canadian Imperial Bank of Commerce (CIBC) and the US-based owner of Winners and HomeSense stores – acknowledged they had lost huge amounts of sensitive personal information." Online: http://www.priv.gc.ca/information/ar/200607/2006_pipeda_e.pdf

[84] OPCC Second ETHI Appearance, to Mr. Wallace, at 10:30.

[85] OPCC Second ETHI Appearance, to Mr. Wallace, at 9:45.

[86] OPCC Second ETHI Appearance, to Mr. Wallace, at 10:30.

[87] Notably, PIAC, CIPPIC (and their *Data Breaches - A White Paper* report, reference *infra*), Murray Long and others. The Privacy Commissioner of B.C., David Loukadelis, recommended against mandatory breach notification.

[88] Recommendations 23, 24 and 25, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA), Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, Adopted by the Committee on April 24, 2007; Presented to the House on May 2, 2007). (ETHI Fourth Report). Online: http://www.parl.gc.ca/content/hoc/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-e.pdf

data breach notification.[89] In effect, Industry Canada called for mandatory notification of individuals only where there was a "high risk of significant harm".[90] There was no such discussion of a harm threshold in the Industry Committee hearings, and the Committee recommended that notification to the OPCC take place in relation to "certain defined breaches of their personal information holdings". It was not totally clear that the Committee had meant this to be when certain defined data elements were compromised, as in the California legislation.[91] Although two witnesses called for consideration of the "sensitivity" of personal information to be considered in deciding whether an organization should have to report a breach to the Privacy Commissioner, there was no "harm standard" suggested by these witnesses other than the implicit assumption in PIPEDA that sensitive personal information is subject to higher levels of protection and care on the part of the organization dealing with the information. Industry Canada simply imported the concept of "high risk of significant harm" from its own work; whether that was sourced politically, bureaucratically, or from consultation is not clear. [92]

Industry Canada also called, however, for removal of the discretion of the Privacy Commissioner to require companies to report breaches to customers.[93] This effectively left the decision about the initial reporting of the breach in the discretion of the company or organization experiencing the breach,[94] on the theory, Industry Canada said, that data breaches must be assessed individually, that the company or organization would be better placed to

---

[89] *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics: Statutory Review of the Personal Information Protection and Electronic Documents Act*. Online: http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/$file/ETHI-e.pdf

[90] *Ibid.*, in Response to Recommendation 23, at p. 10.

[91] A variant of this approach was recommended to the INDU Committee by CIPPIC, who prepared a white paper on data breach for the Committee's review. See: Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper*, January 9, 2007, http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-web.pdf.

[92] PIAC at the publication of the Industry Canada report wrote a response that was highly critical of the Industry Canada report: see PIAC, "Submission to Industry Canada Considering the House of Commons Standing Committee on Access to Information, Privacy and Ethics' Report on the 2006 Review of the Personal Information Protection and Electronic Documents Act (PIPEDA) Public Interest" (January 15, 2008). Online: http://www.piac.ca/files/piac_submission_to_ic.pdf It stated, in part: "PIAC therefore cannot support the Industry Canada position that data breach notification be left to the company or government entity involved to decide, for "certain breaches" (whatever that may mean – presumably "large" – again, whatever that may mean – breaches) based on a threshold of "high risk of significant harm to individuals or organizations". This standard is far, far, far too high and will mean that almost no breaches ever will be reported. It leaves the conflict of interest squarely in place; even voluntary guidelines (backed up with the threat of … what, exactly?) from the OPCC will not change this."

[93] Government Response, *supra*, in Response to Recommendation 24, at p. 11.

[94] Note that Industry Canada also added a caveat to their response – "Assuming appropriate oversight by the privacy Commissioner of Canada" – see next footnote – which suggested that the entire framework of voluntary breach analysis and notification should be predicated upon an "appropriate" level of oversight in general – a large assumption but a critical foundation for their argument in favour of a discretionary regime.

assess risk and harm and that the OPCC might be overburdened by the function.[95] Both Industry Canada and the ETHI Committee also were concerned that a high volume of data breach reports would have the potential to overwhelm the resources of the OPCC.

Interestingly, the Industry Canada response nonetheless appeared to indicate an expectation that organizations that experienced a "major loss or theft of personal information" would in all such "major" cases be required to be reported to the Privacy Commissioner of Canada:

> In addition, as the Committee recommends, a requirement to report any major loss or theft of personal information to the Privacy Commissioner of Canada within a specified time-frame, including the details of the incident and steps taken by the organization to notify individuals (or justification for not doing so), would allow for oversight of organizational practices. This will allow the Privacy Commissioner an opportunity to track the volume and nature of breaches, and the steps taken by organizations respecting the notification process when required. This would be particularly useful to small and medium-size enterprises (SMEs) that may lack the internal resources necessary to make notification assessments.[96]

Industry Canada then undertook a further public consultation on data breach notification and other proposed amendments to PIPEDA on the basis of their reaction to this report in April 2008.[97] Industry members present at the consultations were favourable to the production of data breach guidelines along the lines suggested by Industry Canada, in particular the consideration of notification to individuals only if there was a high risk of significant harm. They also resisted the idea that the OPCC should have any decisive role in deciding if a privacy breach was this serious. This was a matter best left to companies that "know their customers". "Advocacy groups" present at the consultation suggested a lower standard of harm for notification of individuals and took the position that all data breaches should be reported and this number should be reported by the OPCC to the public. Finally, they disagreed with industry

[95] *Ibid.*: "Assuming appropriate oversight by the Privacy Commissioner of Canada, the organization experiencing the breach is well positioned to understand and assess the risks involved and to make a prompt determination regarding whether and how to proceed with notification of their customers, business partners, and/or the general public. Assigning the Privacy Commissioner the responsibility to decide on notification, as proposed by the Committee, would be a less effective alternative, as well as more burdensome for that Office from a resource perspective."

[96] *Ibid.* Presumably "major" breaches would be those creating a "serious risk of significant harm" but it is possible Industry Canada also had an expectation that very large breaches, even without high risk of harm, should at least be reported to the OPCC.

[97] PIAC was present at this consultation and took notes, upon which this paragraph is based.

and stated the OPCC was unconflicted, independent, well placed to, and should, determine which breaches were of significant enough risk to individuals to trigger notification to them.[98]

Regarding the last recommendation of the ETHI Committee, Industry Canada simply repeated the need to develop timing and manner of notification specifics, but studiously avoided the INDU Committee's call for: "penalties for failure to notify".[99] The Industry Canada response also changed the Committee's call for "a 'without consent' power to notify credit bureaus in order to help protect consumers from identity theft and fraud" to "identification of which organizations, such as credit bureaus, should be notified in addition to the Privacy Commissioner."[100]

The PIPEDA review, ETHI Committee report, Industry Canada formal response and government consultations at least had the effect of isolating the issues involved around the two major stages in a data breach notification regime: (1) the initial threshold and criteria for reporting a breach to the OPCC or another privacy commissioner (what we will refer to from this point forward as "administrative notification") and (2) the secondary threshold of determining whether to notify, or require notification to, individuals of the breach of their personal information by the organization in dealing with their personal information (what we will refer to from this point forward as "customer notification").

What seems to have been lost on this journey through the policymaking and legislative process is the voice of consumers.[101] The basic unfairness of having an organization lose the personal information of individuals, then having discretion to even tell them strikes consumers as fundamentally wrong (as quotes below make clear in relation to who should decide whether a report should be made to the privacy commissioner or consumers). This initial wrong seems to get lost in the talk of thresholds, criteria, limits, costs and organizations concerns with the only real result being the refusal to notify consumers.

---

[98] For a list of organizations that participated in consultations, see: http://www.priv.gc.ca/information/guide/2007/gl_070801_org_e.pdf PIAC, Union des consommateurs and the Canadian Internet Policy and Public Interest Clinic withdrew from development of the guidelines in protest of the harm threshold and the discretion left to companies to report to the OPCC in the first place. For PIAC's final written submission on the inadequacy of the proposed guidelines for data breaches, see: PIAC, "Submission to Industry Canada Following the Stakeholder Consultation on the Proposed Model for Data Breach Notification" (April 25, 2008). Online: http://www.piac.ca/files/piac_submission_to_ic_re_pipeda_2008_apr_25_08.pdf

[99] ETHI Fourth Report, *supra*, at Recommendation 25.

[100] Government Response, *supra*, at p. 11, in Response to Recommendation 25.

[101] Bill C-29 got to Second Reading and had one day of House of Commons debate but was not debated at committee. See House of Commons, Debates, 3rd Session, 40th Parliament, 26 October 2010, at 1615 et seq. Even here some MPs expressed concern that the proposed Act was poorly drafted, but comments were general or focused on the controversial new "lawful authority" provisions in another part of the bill.

The OPCC Data Breach Guidelines

Ultimately, since the Privacy Commissioner lacked any order-making power in relation to data breaches, the OPCC settled on voluntary data breach guidelines that it issued August 1, 2007.[102] These had a customer notification threshold of a "reasonable risk of identity theft or fraud" or "a risk of physical harm . . . humiliation or damage to the individual's reputation". While these guidelines were voluntary, they did embody this slightly lower threshold for notification of individuals upon a breach than that suggested by Industry Canada. Gone was the wording "high risk of significant harm", however, present now was the concept that an assessment of potential harm to the individual was to be the main criterion upon which to base an assessment of whether a breach was "major" or serious enough to be reported.

However, there was no suggested requirement in the OPCC guidelines to contact the OPCC or other privacy commissioners. That is, initial administrative notification was not required by the guidelines. Instead it was only "encouraged" under a subsection of the Notification title, "(iv) Others to contact" which states in part:

> **Privacy Commissioners:** organizations are encouraged to report material privacy breaches to the appropriate privacy commissioner(s) as this will help them respond to inquiries made by the public and any complaints they may receive. They may also be able to provide advice or guidance to your organization that may be helpful in responding to the breach. Notifying them may enhance the public's understanding of the incident and confidence in your organization. The following factors should be considered in deciding whether to report a breach to privacy commissioners' offices:
>
> - any applicable legislation that may require notification;
> - whether the personal information is subject to privacy legislation;
> - the type of the personal information, including:
> - whether the disclosed information could be used to commit identity theft;
> - whether there is a reasonable chance of harm from the disclosure including non-monetary losses;
> - the number of people affected by the breach;
> - whether the individuals affected have been notified; and

[102] Noted above. The main document is: *Guidelines - Key Steps for Organizations in Responding to Privacy Breaches*. Online: http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf

- if there is a reasonable expectation that the privacy commissioner's office may receive complaints or inquiries about the breach.

The recommendation then listed other entities to consider notifying such as police and insurers.

Notable in these suggestions and criteria is the introduction of the concept of "material" data breaches – a concept not before clearly discussed at the ETHI Committee nor in the consultations by the OPCC in April 2007.

Bills C-29/C-12

There is no doubt that Bills C-29/C-12 are highly informed by, and based upon the present voluntary data breach guidelines and the history of Canada's present federal data breach notification guidelines. For this reason they promote what is, from a consumer/customer point of view, clearly a weak and likely largely ineffective regime.

Other regimes are not only possible, but are presently in place and operating, both abroad and even in Canada (in Alberta and, for health information only, Ontario and recently New Brunswick and Newfoundland and Labrador). We examine some of these alternative regimes after first examining the scheme proposed under Bills C-29/C-12.

Bills C-29/C-12 are, as noted above, amendments to the present federal-level private sector privacy legislation in Canada, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[103]

Bill C-12, clause 11 creates a new "Division 1.1" in PIPEDA entitled "Breaches of Security Safeguards". As noted above, this framework for data breach regulation is that currently used in the U.S. and seems to be intuitively that which may be conceptually most understandable to the public. However, this is where similarity with the U.S. and indeed most other data breach legislation and even voluntary codes ends.

Administrative Notification

New section 10.1 of PIPEDA is introduced by this Bill. It is the bill's description of the administrative notification requirement (the requirement on the organization to report to the Office of the Privacy Commissioner of Canada). The first subsection language appears mandatory and prescriptive:

[103] S.C. 2000, c. 5.

> 10.1(1) An organization shall report to the Commissioner any material breach of security safeguards involving personal information under its control.

Unfortunately, the "material breach" requirement in subs. 10.1(1) is defined in new subsection 10.1(2) in a way that makes it virtually impossible for a breach ever to be judged material, for two reasons. First, the section contains a criterion that, if admitted by the organization, is tantamount to an admission of liability or at least is an admission of negligence in relation to its data handling processes; and second, the assessment of this criterion is to be judged by the organization itself and not on an objective standard.

The wording of the materiality requirement in new s. 10.2 reads:

> 10.1(2) The factors that are relevant to determining whether a breach of security safeguards is material include
>
> (a) the sensitivity of the personal information;
>
> (b) the number of individuals whose personal information was involved; and
>
> (c) an assessment by the organization that the cause of the breach or a pattern of breaches indicates a systemic problem.

Even if the first two requirements (sensitivity of the information and number of individuals involved) is to be adjudged on an objective standard, the subsection requires (note the connecting word "and") that the organization assess, internally and subjectively, whether the breach (or pattern of breaches) indicates a "systemic problem". No organization, in particular in a situation that could lead directly to lawsuits against it based on its corporate data security standards and practices would admit that it indeed did have a "systemic problem" that the breach brought to light. Even if the internal assessment of the organization was that the breach did reveal a systemic problem, it would be the poorest of corporate management, brand management or risk management to admit that fact outside the organization. This criterion is thus a one way incentive to non-reporting. It leaves all discretion and judgment in the hands of the organization that has many other strong incentives not to report. It is remarkable besides its completely predictable effect not only in that it encourages non-reporting but also in that in the entire world of data breach regulation, including statutory and voluntary regimes, there is no similar provision which at the same time both presents an organization with a risk hurdle to consider that will only harm the organization while at the same time offering clear path around that hurdle by permitting a self-serving assessment that the organization is not negligent.

That this provision will instantly be used by organizations in a regular way as a "get out of reporting free" card seems likely. Indeed, PIAC has already been present where a

representative of a major Canadian telecommunications corporation, in discussion of the new administrative reporting requirement under Bill C-29, with representatives of two privacy commissioners on a panel, replied in response to a hypothetical fact situation of a potential credit card breach that the breach did not implicate the company's corporate security at the "systemic" level. Thus it was suggested that the corporation would not report the breach to the privacy commissioner, even after the scenario was extended to a different but related breach of credit card data, as the representative stated it was not necessarily systemic.[104] The privacy commissioner representatives, however, even before the first fact situation was extended to include a second breach, stated it was possibly systemic, and emphasized the difficulty of determining this if there were no audit trail for computer or network accesses to personal information. In short, it was practically impossible for the regulator to conclude a single situation, or even a series of situations, was evidence of a systemic problem and the corporate representative indicated in any case that these were not systemic. This panel is shocking from a consumer perspective but understandable from a corporate one; indeed, a corporate lawyer likely would rely upon an interpretation that such incidents were unique and unrelated as a clear and obvious path to avoid potential liability, cost to the organization of reporting and potential reputational damage. From a privacy commissioner perspective, it indicates the legislation's main reporting criterion is based almost wholly on information that is almost entirely in the possession of the organization and may be missing due to a lack of internal audit mechanisms and, in any case, the organization has complete control of even revealing that information, based on its own self-interested assessment of how "systemic" the problem is.

The OPCC seems content with the idea that organizations in the conflict of interest position they find themselves make this initial determination of whether the breach is "material":

> We feel the legislation takes a reasonable approach in having private-sector organizations make the initial determination as to whether consumers need to be notified of a breach. Our Office would retain the authority to investigate a data breach or recommend to an organization that it notify affected individuals if we feel that's appropriate.[105]

[104] Canadian Bar Association conference "Privacy Rights in the Age of Technology" The State of Canadians' Information Rights in 2010 and Beyond", September 19-20, 2010, Sheraton Ottawa in the panel "Anatomy of a Data Breach", in particular Case Study #2, found at Appendix 3.

[105] "Protecting Privacy in the Age of Big Data: Change, Challenges and Solutions - Remarks to the Council of Chief Privacy Officers organized by the Conference Board of Canada" Speech by Chantal Bernier, Assistant Privacy Commissioner of Canada, January 25, 2011. Online: http://www.priv.gc.ca/speech/2011/sp-d_20110125_cb_e.cfm

What is not clear is how the OPCC would be able to investigate breaches that the organization, in its own unreviewable discretion, sought not to report to the OPCC.

In short, the administrative notification threshold seems designed to deter an organization from ever reporting a data breach.[106] The section appears to contradict the policy goal of the act, and while giving the impression of requiring organizations to report data breaches, instead authorizes them to avoid this unpleasant result.

Customer Notification

As noted above, the OPCC guidelines require a certain level of risk to be present before the corporation is encouraged to report the breach directly to customers, who are the ones who ultimately may face threats like identity theft, fraud and stress and inconvenience associated with the loss of their personal information.

Recall also that the threshold initially suggested by Industry Canada was a "high risk of significant harm" to the individuals. This standard was modified some time in 2008 in a "model statute and commentary" which was provided to some but not all stakeholders.[107] The new suggested standard was "substantial risk of significant harm". This standard still would seem to require a risk was more likely than not to be realized.

Bill C-12 repeats the requirement of a harm-based test for reporting data breaches directly to affected individuals. Bill C-12's requirement is found in new subsection 10.2(1). It reads:

> 10.2 (1) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the

---

[106] See the comment on this requirement (in Bill C-29) by Philippe Neray, VP Security Strategy, Guardium, an IBM company, "Canada's newly introduced data breach law is a start, but it lacks teeth," SC Magazine, July 08, 2010 (online: http://www.scmagazineus.com/canadas-newly-introduced-data-breach-law-is-a-start-but-i/):

> In other words, the bill states that companies have the right to determine *whether to even disclose a breach* based on the type of information stolen, number of customers affected and whether the company thinks there's a real risk of significant harm to the individual(s).
>
> In comparison, U.S. state laws stipulate mandatory disclosure *whenever* personal information has been acquired by an unauthorized person, or whenever there is risk of any harm (not just "significant harm"). Also, unlike C-29, which contains no clear penalties for failure to disclose a breach, U.S. state laws also establish harsh monetary penalties for failure to promptly comply (such as up to $750,000 in Michigan).

[107] ULCC, Report 2010, infra, at p. 5 cites in a footnote this reference "Industry Canada,"A Model for Data Breach Notification Reporting and Notification under the Personal Information Protection and Electronic Documents Act", June 2008." PIAC did not obtain a copy.

> circumstances to believe that the breach creates a real risk of significant harm to the individual.

The new harm threshold now is expressed as a “real risk of significant harm”. Once again, as with the administrative notice section, subsections 10.2(2) and (3) of the customer notification section attempts to define the key parts of this test.

First, subs. 10.2(2) creates a non-exhaustive list of factors that can be considered as "significant harm". They are: "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." These are largely the same as those in the OPCC voluntary data breach guidelines with the addition of credit record effects and damage to property or loss of property.[108]

However, it is in subs. 10.2(3) that the term “real risk” is defined, or is at least given certain legal parameters, referred to as “relevant factors”:

> (3) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include the following:
>
> (a) the sensitivity of the personal information involved in the breach; and
>
> (b) the probability that the personal information has been, is being or will be misused.

While at first blush, these factors appear to militate towards notification in most cases, the fact is that the assessment, even if done on a reasonable person standard, leaves the organization that suffered the breach to make this determination. That is, the organization that lost the information will decide its sensitivity to the person whose information was breached. The second half of the test, (b), the “probability that the personal information has been, is being or will be misused” likely is out of the realm of knowledge of a self-interested organization that is trying to control a data breach. In fact, the “natural” or usual corporate response is to attempt to reassure customers that nothing bad can come of a breach.

---

[108] The potential harms were stated in the federal guidelines in this manner:

> What harm to the individuals could result from the breach? Examples include:
> o security risk (e.g., physical safety);
> o identity theft;
> o financial loss;
> o loss of business or employment opportunities; or
> o humiliation, damage to reputation or relationships.

There is no absolute nor really any relative way of making the determination of the likelihood of misuse. In many of the decisions under the Alberta data breach law, the Commissioner relied upon the fact that, even when information was recovered fairly quickly and access likely was fairly limited, there was in fact no way for the organization to know if it had been accessed and was likely to cause harm or not. This provision of Bill C-12 therefore calls upon self-interested corporations to gaze into their crystal balls to see if the future bodes ill for their customers.[109]

Focus group members thought that that decision about how data was likely to be misused or how sensitive it is was more a subjective question than an objective one and that there was a clear risk that an organization would not understand the concerns of a potentially large minority of its customers' sensitivity to losing particular data elements.[110]

It thus bears repeating: under Bill C-12 the federal OPCC has no formal role in making either of the determinations that could lead to a finding that there was a "real risk of substantial harm" that should have required notification. An organization, even if it had reported the breach to the OPCC, has no duty to consult with the OPCC's view of sensitivity nor probability of misuse and may proceed under this bill on its own assessment.

The result of the definitions in Bill C-12 seems certain to sink the chance of virtually all but the most publicized data breaches from ever triggering a notification to customers.

---

[109] See Calgary Focus Group 2 at p. 51:

> R: …I think it should be up to a third party to make that decision, how serious it is. Because the company could look at something and say, ah, that's not so serious, let's wipe that under the rug, where the third party who has no interest could say, no.

[110] See Calgary Focus Group 1 at pp. 24-25:

> R: But see, every individual, like you were saying, who decides, number one, what … you think, oh, that's okay, they've got my name. But I don't think it's okay. So I think individually …
> R: It's very subjective.
> R: Yeah.
> M: Bernard, what do you think?
> R: Well, yeah, that's what I'm saying. Who makes that decision whether or not it's inconsequential or it has some serious impact? Because it is an individual decision in terms of what I consider is my close personal information and what information I want out there in the void, or not.
> M: There are things you might consider confidential that other people would tell the world.
> R: And the other way around. There's something that I might consider inconsequential and someone else says, geez, why did you put that out there? But who is going to make that decision, okay, we don't need to notify them because this is of no matter? Well, maybe it matters to 20% of that database, and they should be notified. Maybe what they need to look at is notifying everybody but doing it at, shall we say, different stages or different levels. If it's a "relatively insignificant breach", like a name was slipped but there was no other personal information, you can send them a letter. But if there was something of any serious consequence, then maybe you need to step it up and contact these people relatively quickly.

Despite this, most stakeholders seem content with, or are oblivious to, the entrenching of a regime that seems designed to hide data breaches, rather than to notify affected customers.

The Uniform Law Conference of Canada had in a draft uniform law from 2008 and an interim report in 2009 suggested instead a customer reporting threshold of "a risk of significant harm". However, "[t]his was criticized by some private sector interests as too weak a test, i.e. one that would require notification even if the risk were hypothetical or speculative." The ULCC reacted by retreating from their more favourable position for notification.

The ULCC in a subsequent August 2010 report that cites the C-29 test of "real risk of significant harm" stated that:

> [11] Industry Canada published a model statute and commentary in 2008 as well, in which the test was "a substantial risk of significant harm." The Privacy Commissioner of Canada criticized this proposed test as too rigorous, in that it would allow too many breaches to go without notice, and too much risk would accrue to the individuals whose information was improperly accessed. No doubt the phrase "a real risk" was meant to be a compromise between these two concerns.
>
> [12] The Working Group recommends adopting the Alberta/federal language as the appropriate test for notification: a real risk of significant harm. This seems right in principle and also may turn out to be a trend, or at least widely acceptable as a matter of policy. Using this language probably maximizes the chance that the uniform statute will be adopted.[111]

While one of the goals of the ULCC is to attempt to harmonize provincial and indeed federal laws, it is neither the only nor paramount goal. Nonetheless, it appears by virtue of repetition in the Alberta PIPA and federal bills, this phrase likely will be accepted as a fair standard. Thus it is to the interpretation of the standard that we now turn.

The Privacy Commissioner of Canada has not since Bills C-29/C-12 commented substantively on the appropriateness of a "real risk of significant harm". Instead, the OPCC has made general references to the standard, and in one speech has averted to the difficulty of its interpretation:

> Without getting into the fine details of statutory interpretation, suffice it to say that the thresholds which trigger a reporting obligation to the Commissioner and/or a notification obligation to the individuals affected vary from law to law.

[111] ULCC, UNIFORM PROTECTION OF PRIVACY ACT (DATA BREACH NOTIFICATION), Identity Theft Working Group, REPORT 2010 (Halifax: August 2010), at paras. 10-11 [footnotes omitted]. Online:

> A discussion about what constitutes a "material breach" or a "real risk of significant harm", for example, could be the subject of a whole other hour.

It is unfortunate that the OPCC has not attempted to enlighten the public and privacy lawyers and advocates as to the way it will interpret this key provision. Perhaps this is because, under the Bill, the OPCC has only an oversight, if not bystander, role.

While "real risk" may be meant to indicate a lower possibility of harm than the previous "significant risk,"[112] both formulations appear to pose a difficult challenge in assessing the risk to consumers. This approach may produce increased risk for consumers with subjective concerns or circumstances if they are not taken into account by the organization, such as: previous difficulties with identity theft; poor or fragile credit scores or reports; or for those with fewer financial resources or facility to resolve problems (such as those with low literacy or cognitive disabilities) or youth, as noted in the focus groups:

> M: What about the circumstances of the breach? Like for example, if the information lost is that of a teenager or a child. Does that make any difference? Does that make it any more or less serious?
>
> R: It's still as valid.
>
> R: Depending on the information. Like if you're speaking their shopping patterns, if someone knows my kid buys shoes and shirts and pants three times a week …
>
> M: Right, and they probably don't have much in their bank account.
>
> R: Big deal, yeah. But I mean other information might be more sensitive.[113]
>
> . . .
>
> M: By the way, when we talk about data breaches, does the circumstance of the breach matter? For example, let's say that the information that's been breached is that of a teenager or a child, does that make it any more or less serious than if it was an adult?
>
> R: Wouldn't it be equal?
>
> R: I think so. I wouldn't want my kid's information out there any more than I would want my own.

[112] Several Alberta IPC decisions have interpreted a low risk of harm as "real" if the potential effects are very serious. See, for example, Alberta, P2010-ND-001 (the Knights of Columbus Order).
[113] Calgary Focus Group 1 at pp. 32-33.

R: M'hmm.

R: All my kids have scholarships and they all have a social insurance number to have that scholarship. That's still information that they could steal from a 13-year-old boy and it might not affect him the same way it would affect me but I think on the whole it would affect the family.[114]

The abstract assessment by the breaching organization of the likelihood of misuse for the majority of customers also simply can be wrong. The abilities of those stealing or acquiring personal information may well be far more advanced than suspected by a "reasonable" person or organization with average security knowledge. The focus group participants in particular mentioned this in relation to organizations' faith in encryption or redaction of data:

M: What if the company or institution claims that the information … Let's say that there is a data breach but the company says, well, the information has been de-identified or anonymized or encrypted somehow. So, yes, there was a data breach and technically some of your personal information is there but it was encrypted in a way that nobody who found it would be able to do anything with it.

R: Well, there is a … people can do stuff.

R: It's never foolproof.

R: Exactly.

R: There's a level of hackers, I think they can breach anything they want. If they have the data and it's encrypted it's just a matter of time.

R: With enough time and know how you can always de-encrypt things.

R: If they have the motivation to do so.[115]

Focus Groups Participants Views of the Administrative and Customer Notification Thresholds

The four focus groups conducted by PIAC discussed both the administrative and customer notification thresholds extensively. In short, nearly all participants thought leaving the administrative notification decision to the organization having the breach would expose them to serious risk.

[114] Calgary Focus Group 2 at p. 28.
[115] Calgary Focus Group 2 at p. 30.

M: It was not very well publicised, obviously, because nobody seems to have heard of it. In any case, there is a law and it says that, if there's a breach, a data breach, the company has to notify the Office of the Information and Privacy Commissioner for Alberta, OIPC. They notify them if the company thinks that there is a real risk of significant harm and the company must assess if a reasonable person would consider the breach to create real risk of significant harm to individuals. So, in other words, they don't have to report all data breaches. They have to report all data breaches that they think a reasonable person would consider to create a real risk of significant harm.

R: So, it's the company that is ultimately deciding if the data breach is serious.

M: Yeah. So, what do you make of that?

R: Is reasonable, but it's missing out what we were all just talking about.

M: Which is?

R: Just that if they don't report it and something goes on, that nobody where that came from. If they reported all breaches then somebody at the other end could file away all the minor ones and …

R: Do a triage of them.

R: Exactly, yeah.

R: I think it should be up to a third party to make that decision, how serious it is. Because the company could look at something and say, ah, that's not so serious, let's wipe that under the rug, where the third party who has no interest could say, no.[116]

The focus group members also felt the same unease at leaving the decision of whether to notify customers in the hands of the organization suffering the breach:

M: I guess maybe part of the question is, when it comes to deciding whether a breach is serious enough that everyone should be notified, should we trust the companies to decide whether it's serious enough, or should there be some third-party that decides whether it's serious enough?

R: For sure it has to be a third party.

[116] Transcript Calgary Group 2, p. 51.

R: Yeah.

R: Effectively that's why we have government or whatever body who sets these rules out and the companies abide by them, or not, but it doesn't make sense to have the company … To me it doesn't make sense to have the company, because again, it's a conflict of interest. It's like, well, it might have been a breach there but, aah yeah, it's fine. So, I think you have to have a third party.[117]

...

R...Yeah, it's very vague, and you have companies that, some companies are going to be responsible and some … that's the reason we still have labour laws. You know, there are some companies that just can't do it by themselves, you've got to police them from top to bottom.[118]

Some focus group participants in Montreal also questioned potential harm as a standard and viewed the organizations as having something more of a stewardship role over their personal information, or even a duty of confidentiality.

M. [. . .] Donc ce que je veux savoir c'est croyez-vous que les consommateurs comme vous autre devraient être informés de toutes les violations de données quelque soit leur gravité ou y a-t-il un inconvénient à cela?

R : Comme disait D. tantôt, moi je me demande si les institutions se protégeraient en faisant ça ou si ça serait les consommateurs que ça protégerait?

R : Mais je pense qu'il y a une obligation morale de le faire, mais ils le font pas parce que les conséquences dépassent ce que ça a comme inconvénient.[119]

Comments from the focus groups were largely consistent that there was an insurmountable conflict of interest in an organization that had suffered the breach having any real role in deciding whether to report to a privacy commissioner or to customers.

[117] Calgary Focus Group 2, September 15, 2010 – 8:00 p.m., at p. 33.
[118] Calgary Focus Group 1, p. 65.
[119] Montreal Focus Group, 9 September 2010, at 17:30, at p. 24-25.

Alberta PIPA

The Alberta *Personal Information Protection Act* (PIPA) does notification in a different way than the federal bill and federal breach guidelines, with however, some of the same definitional tools.

What is different in the Alberta law is the emphasis on reporting by the organizations to the privacy commissioner, then the required determination by the privacy commissioner if the breach should be reported to affected customers. Frank Work, in the latest Alberta OIPC Annual Report, stated that in doing so, the office would be taking a risk, but the risk would have definite consumer advantages:

> In 2009, following a legislative review of PIPA, amendments were made to PIPA in which Alberta became the first jurisdiction in Canada to adopt mandatory breach notification. During the legislative review, the OIPC specifically asked the Select Special Committee to recommend requiring organizations to report losses of information to the Commissioner and to give the Commissioner the power to decide whether or not there should be notification to affected persons. The OIPC knew it was risky: the OIPC was, in effect, setting ourselves up as insurers. If we decided there was no real risk of significant harm and therefore no need to notify, and people did get harmed, the blame would fall to the OIPC. But having the Commissioner do it would make for more uniform reporting, more consistent application of the standard (real risk of significant harm) and better notification where notification was required. Furthermore, people would be spared a steady stream of spam-like notices for minor losses.[120]

Besides the benefits of consistency and focus, notably for consumers, however, the Alberta model produces more reporting of data breaches.[121]

Alberta achieved these results by, in its PIPA law, placing the consideration of "real risk of significant harm" into an objective test at the administrative notification stage.[122] That is, an organization must consider, on a reasonable person standard, if the breach would result in a

---

[120] Office of the Information and Privacy Commissioner of Alberta, 2010−11 ANNUAL REPORT at pp. 5-6. Online: http://www.oipc.ab.ca/Content_Files/Files/AnnualReports/AR_2010_2011.pdf

[121] Since the introduction of data breach notification in 2010, the Alberta Privacy Commissioner has made 31 orders to notify individuals (11 in 2010; 20 thus far in 2011) and has received at least 97 administrative data breach notifications from the organizations holding information on Albertans.

[122] *Personal Information Protection Act*, S.A. 2003, c. 6.5, section 34.1(1): "34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure."

"real risk of significant harm". If so, the organization must report to the Office of the Information and Privacy Commissioner of Alberta. The Alberta OIPC also had general order making power, unlike the federal Privacy Commissioner, prior to the amendments to PIPA providing for data breach notification. Therefore, the Alberta legislature saw no impediment to providing a specific order-making power to the Alberta Privacy Commissioner to order, after administrative notification to it, the customer notification, even against the wishes of the organization.

The effect of moving the harm standard to the first stage of the test, as noted, appears to result in more customer notification. However, this is less likely due to organizations considering the fine points of the harm standard and more to do with placing a purely objective "reasonable person" standard for reporting at this stage. In addition, organizations no doubt are aware that Alberta PIPA prescribes a fine of up to $100,000 for organizations and $10,000 for individuals for not reporting a breach to the Commissioner that objectively does create a real risk of substantial harm.[123]

Finally, the Alberta Privacy Commissioner has taken the approach that "real risk of significant harm" can be interpreted to capture most data breaches and therefore require notification. The Alberta Commissioner set the tone in several early breach notification decisions.

Several notification decisions have been made by the Alberta Privacy Commissioner under the Alberta *Personal Information Protection Act*. They tell a tale of reluctance to notify on the part of organizations and a corresponding need for powers in the Commissioner to order that notification to individuals be undertaken more rapidly.

For example, the very first data breach notification order of the Alberta OIPC was regarding a breach suffered by the Knights of Columbus in the United States. However, nine Alberta residents were affected. The Alberta Commissioner ordered notification, despite the fact that the Knights of Columbus stated the information involved (hard copy records found in a dumpster, and some missing or moved electronic records) was not likely to create a "real risk of significant harm". Commissioner Work started from the proposition that since the Knights of Columbus could not vouch for the whereabouts of the personal information nor that it had not been accessed and then dumped, the breach was a real risk of significant harm to the Alberta residents. His reasons illuminate a "customer first" line of thinking that accepts that there may be harm when a risk has been demonstrated, absent a strong reason to believe all is well:

> [17] In order for me to require that The Knights of Columbus notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to individuals as a result of the incident; moreover, that harm must be

[123] PIPA, section 59(1)(e.1).

> "significant" – it must be important, meaningful, and with non-trivial consequences or effects.
>
> [18] In this case, the personal information at issue is of moderate to high sensitivity as it includes names, addresses, Social Security numbers, financial account numbers, drivers' license numbers, medical and/or other personal information of individuals.
>
> [19] This is information that could be used to cause significant financial harm to individuals, and provides comprehensive individual profiles that could be used for identity theft and/or fraud.
>
> [20] In order for me to require The Knights of Columbus to notify individuals, however, there must also be a "real risk" of harm to individuals as a result of the incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.
>
> [21] I note that the length of time the information was exposed in this case was relatively short; that is, The Knights of Columbus determined that the incident must have occurred within a few days of the organization being notified and, upon being notified, took steps to immediately recover the information, and believes most of it was recovered.
>
> The Knights of Columbus also reported that it does not believe there to be a real risk of harm to the affected individuals. However, at this time, and despite ongoing investigation, the cause of the incident is still unknown. The whereabouts of the additional files is also unknown, as is the cause of their disappearance, and the length of time they have been missing.
>
> [22] Given the sensitivity of the information at issue, and considering that it is not known whether the files were inadvertently disposed of by a careless employee, or alternatively, accessed by someone with intent to cause harm, I believe there to be a real risk of harm in this case.[124]

Notable in this quote (at para. 20) is the setting of what appears to be the Alberta IPC's legal definition of a "real risk" of significant harm. The elements required are: 1. a risk that exists

[124] Alberta OIPC, Breach Notification Decision No. P2010-ND-001, *The Knights of Columbus Charitable Foundation*, Case File #P1631 (August 9, 2010). Online: http://www.oipc.ab.ca/Downloads/documentloader.ashx?id=2684

("more than mere speculation or conjecture") but that may be less likely than not; and 2. causation.

The Alberta OIPC in its latest Annual Report[125] noted the large increase in reporting of data breaches since amendments to PIPA came into effect in May 2010:

> The number of Self-reported Breaches increased significantly this fiscal year, given the amendments to the PIPA which require organizations to report incidents where there exists a real risk of significant harm to an individual. The Act also empowers the Commissioner to require organizations to notify individuals to whom there is a real risk of significant harm as a result of such an incident. These ground breaking amendments to PIPA came into force on May 1, 2010 and are the first such law in Canada. Forty-nine (49) new cases were opened when organizations self-reported privacy breaches. This represents a substantial increase of over three times the number of reported breaches compared with the previous fiscal year (15 breaches were self-reported in 2009-10).[126]

Reading between the lines of the latest Annual Report somewhat, it is possible roughly to determine the ratio of reports to the Alberta OIPC and the mandatory orders to report to customers. The data breach decisions published on the website are most cases where the organization disagreed with the OIPC and did not want to report, but was overruled by the OIPC (in a very few cases, the OIPC agreed proper notification was done and no further notification was necessary):

> A total of 49 breach notification decisions were issued by the Commissioner during the fiscal year of 2010-11. Of these decisions, 17 breach notification decisions were published as only those decisions in which the Commissioner requires that an organization notify individuals to whom there is a real risk of significant harm are posted on the OIPC website at www.oipc.ab.ca.[127]

Therefore the ratio of orders to the opinion that no notification to customers was needed was in the range of 1:3. These numbers do, however, include situations where the organization voluntarily reports to customers but may be ordered to report to a wider number or was in the process of notifying when the order came out. These voluntary numbers appear to be included in overall breach notifications to the OIPC, however. This is what Commissioner Work had to say about the volume of data breach notifications in his "Message from the Commissioner" in the 2010-11 Annual Report:

---

[125] Office of the Information and Privacy Commissioner 2010-2011 Annual Report and Audited Financial Statements. Online: http://www.oipc.ab.ca/Content_Files/Files/AnnualReports/AR_2010_2011.pdf
[126] *Ibid.*, at p. 15.
[127] *Ibid.*, at p. 17.

> Since breach notification came into force on May 1, 2010, we have had 97 breach notifications. We are now processing about 8 reports a month. We do not have enough resources to handle this increased caseload. From what I have seen from the breaches reported to date, it may be time for the Government to consider legislating penalties where reasonable security measures were not taken and information was lost as a result.

This real-world experience indicates that there is likely a large number of data breaches by organizations happening across Canada every year, probably in the hundreds, possibly in the thousands. It also indicates that even when presented with a fairly clear test of harm, organizations are, or would argue for, not reporting to customers. Therefore, it is likely, depending on the definition of data breach that many consumers and customers may not receive a notification even under a fairly strict regime (at least until they are so ordered).

Content of Notices

Provided a notice is to be given under an act or guidelines, there generally are formal requirements as to what information should be so provided either to the relevant privacy commissioner, or to the customer. Notice requirements should serve the dual purpose of communicating all information that will be needed by the recipient with clarity and concision, to avoid communicating needless or confusing information, and to allow the notifying organization to quickly and efficiently prepare accurate notices based on a template.

Intuitively, this would mean that requirements for such notices should be laid out in some detail, although leaving room for particular circumstances. That is, they should be specific enough to provide guidance to the sender and the recipient, and to avoid excessive generalities that might lead to vastly varying notices in which the sender is given excessive latitude to describe (or not) the circumstances of a data breach.

Notices should also be appropriate to the audience. A notice to a customer will concentrate on explaining what happened and what a customer can do to mitigate potential losses. A notice to a privacy commissioner will concentrate on the number of records and nature of the data lost. A notice to other third parties (which we call "third party notices" to avoid confusion with "administrative notices") such as sub-contractors dealing with the data; credit bureaus; police and insurers; all will be tailored to the function that those third parties play in a data breach.[128]

[128] See the discussion of the various audiences for notices, including consumer, regulator and industry, and the three functions of notice regimes: lessons learned (for industry sectors or as a whole); "repairing" consumer harm; and punishment (via "name and shame") of those organizations in Andrew Cormack, "Data Breach Notification: Purposes and Incentives" Draft 0.05 (15 June 2010) ©2010 The JNT Association Ltd. Online: http://www.ja.net/development/legal-and-regulatory/related-regulatory-

Focus group comments on notices emphasized the need for help or explanation of what customers should do about the breach, for example, get their credit report.

> M: Should the notification describe in detail what data was lost, like, tell you, these are the pieces of information that were …?
>
> R: Yeah, that's your personal information.[129]
>
> ….
>
> M: What are the kinds of things they could tell you to do, do you think?
>
> R: Dummy-proof it, pretty much. That way you're not scrambling and trying to figure out, okay, I need to get this replaced, this, this, this. It's just, okay, you need to …
>
> M: You don't necessarily need to get anything replaced at all. They may just tell you, you need to be vigilant around …
>
> R: Yeah, preventative, I guess.
>
> R: Or, watch these things in the future in case something comes up.
>
> R: Yeah.[130]

Administrative Notices

Bill C-12 does not specify, at this time, what details the notice to the OPCC should contain. Instead, Bill C-12 leaves the definition of these matters to the regulation, which as yet has not been proposed along with the Bill.

---

documents/Data%20breaches%20draft%20v0.05.pdf PIAC does not agree with the conclusion of this paper that " It is therefore unlikely that any mandatory breach reporting scheme can achieve more than one of the purposes. Any scheme that attempts to combine them is likely to fail in its objectives, damage public confidence in digital storage of information, and may even become itself a threat to privacy if information shared for one purpose is used for another." We believe all three purposes can be balanced and self-reinforcing - see Conclusions - New Approach is Needed.

[129] Transcript Calgary Group 2, p. 39.

[130] Transcript Calgary Group 2, p. 40.

Unfortunately, at the present time at the federal level, there are only the OPCC guidelines, which, since they do not mandate disclosure to the OPCC, only really provide guidance to organizations about what to provide to customers for a customer notification.

As a result, it is more useful to examine the approach in Alberta, under Bill C-12 and in some U.S. states that have data breach requirements already in place.

Alberta

The Alberta PIPA likewise to Bill C-12 does not place the administrative notification requirements in the Act but instead in regulations. The administrative notification requirements are quite detailed, covering details of the breach that the privacy commissioner would need to know to order customer notification if necessary and to determine the manner of that notification.[131] In short, the regulation requires information to be provided to the privacy commissioner in enough detail to evaluate the breach.

Customer Notices

Under Bill C-12

Under Bill C-12, the formal details of the breach notice could be specified in regulations, which are as yet not proposed. However, the bill does require that:

> (4) The notification must contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are

[131] See *Personal Information Protection Act Regulation*, AR 366/2003, as am., s. 19, which reads:

> *Notice to the Commissioner*
> 19 A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include the following information:
> (a) a description of the circumstances of the loss or unauthorized access or disclosure;
> (b) the date on which or time period during which the loss or unauthorized access or disclosure occurred;
> (c) a description of the personal information involved in the loss or unauthorized access or disclosure
> (d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;
> (e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;
> (f) a description of any steps the organization has taken to reduce the risk of harm to individuals;
> (g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure;
> (h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.

> possible, to reduce the risk of the harm that could result from it or to mitigate that harm, as well as any other prescribed information.

What constitutes "sufficient information" to "understand the breach" and "take steps ... to reduce the risk of the harm ... or mitigate that harm" is potentially a valuable addition to the data breach regulatory ethos. At present, as we detail below, in most legislation and guidelines, there are only weak requirements to explain the breach in any intelligible detail and very little to encourage organizations to create notices that help customers by suggesting steps of action.

Our focus groups indicated they would expect, and welcome, such suggested actions as they might not know the significance of a notice, nor what to do if they received one.[132]

One example of where legislation tries to address these concerns is in the U.S. state laws. For example, in Iowa,[133] Maryland,[134] Missouri,[135] North Carolina[136] and Oregon,[137] a notice must contain "Contact information for consumer reporting agencies" or "toll-free numbers and addresses for the major consumer reporting agencies." This is in addition to a requirement in most states to contact the credit bureaus directly when 1000 or more of a state's residents are affected.

North Carolina provides a potential list of what Bill C-12's "sufficient information" might look like. North Carolina requires:

> Notice must be clear, conspicuous, and shall include all of the following:
>
> • A description of the incident in general terms;
>
> • A description of the type of PI that was subject to the unauthorized access and acquisition;
>
> • A description of the general acts of the business to protect the PI from further unauthorized access;
>
> • A telephone number for the business that the person may call for further information and assistance, if one exists;

[132] See above comments of the focus group participants, in relation to content of notices.
[133] Iowa Code § 715C.1-2.
[134] Md. Code Com. Law § 14-3501 et seq.
[135] Mo. Rev. Stat. § 407.1500.
[136] N.C. Gen. Stat. § 75-65.
[137] Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626.

• Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;

• The toll-free numbers and addresses for the major consumer reporting agencies; and

• The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the NC AG's office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

It is notable that these types of information were mentioned in our focus groups. These types of information are meant to directly address potential consumer apathy towards the notice and to offer resources and support to dispel consumer anxiety and confusion.

It is up to legislators to determine the regulations under the C-12 content of notification requirement, however, the North Carolina list appears to be well-aligned with consumer expectations and should be studied as a possible best practices for notices.

Federally - Guidelines

The federal data breach guidelines are fairly detailed as to the types of information that could appear in a consumer notice, however, the guidelines are voluntary and leave scope for a wide variation in the type and amount of information that could be provided to consumers under the guidelines. Nonetheless, these guidelines include valuable, consumer-centric suggestions.

For example, the notification suggestion includes the following list:

> The content of notifications will vary depending on the particular breach and the method of notification chosen. Notifications should include, as appropriate:
>
> • Information about the incident and its timing in general terms;
>
> • A description of the personal information involved in the breach;
>
> • A general account of what the organization has done to control or reduce the harm;
>
> • What the organization will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. Possible actions include arranging for credit monitoring or other fraud prevention tools, providing information on how to change a social insurance number (SIN), personal health card or

driver's licence number. For example, to obtain a new SIN see http://www1.servicecanada.gc.ca/en/cs/sin/0200/0200_010.shtml;

• Sources of information designed to assist individuals in protecting against identity theft (e.g., online guidance on the Office of the Privacy Commissioner's website http://www.priv.gc.ca/resource/ii_4_01_e.cfm and Industry Canada website at http://strategis.ic.gc.ca/epic/site/oca-bc.nsf/en/h_ca02226e.html

• Providing contact information of a department or individual within your organization who can answer questions or provide further information;

• If applicable, indicate whether the organization has notified a privacy commissioner's office and that they are aware of the situation;

• Additional contact information for the individual to address any privacy concerns to the organization; and

• The contact information for the appropriate privacy commissioner(s).

Be careful not to include unnecessary personal information in the notice to avoid possible further unauthorized disclosure.

Many of these elements were requested by the focus groups as being helpful or necessary resources after they had read the notice.

Alberta

Alberta, in its regulation to PIPA, s. 19.1,[138] lays out the customer notice formal requirements:

> 19.1(1) Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must
>
> (a) be given directly to the individual, and
>
> (b) include
>
> (i) a description of the circumstances of the loss or unauthorized access or disclosure,

[138] See *Personal Information Protection Act Regulation*, AR 366/2003, as am., s. 19.1.

(ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,

(iii) a description of the personal information involved in the loss or unauthorized access or disclosure,

(iv) a description of any steps the organization has taken to reduce the risk of harm, and

(v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.

What Alberta's regulation does less of is provide information on "what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves." However, this is precisely the information the focus group participants (in both Alberta and Québec) felt would be one of the most valuable features of such a notice:

M: Now the content, by the way, if you get a notice in Alberta, and given that you all live in Alberta, if you did get notified here's what you're supposed to be told. A description of the circumstances of the loss or unauthorized access of disclosure; the date on which or time period during which the data breach occurred; a description of the personal information involved in the loss; a description of any steps the organization has taken to reduce the risk of harm to individuals; contact information for a person who can answer on behalf of the organization questions about the loss. Is this enough, or is anything missing?

R: Steps you can do.

R: Steps you can do, yeah.

R: Was that in your list?

M: No.

R: Oh, okay. So, yeah, you need to know how to follow up on your behalf. Or if there is nothing you can do, then you need to be assured there is nothing you can do. [139]

...

[139] Transcript Calgary Group 1, pp. 69-70.

R: J'aimerais savoir d'abord est-ce qu'il y a des actions qu'il faut que je prenne pour me protéger ou qui je dois appeler dans la compagnie parce que souvent on me dit que l'information qui est une fraude sur la carte, mais qui je dois appeler et j'aimerais ça qu'ils me donnent les étapes qu'il faut que je prenne pour avoir ma carte rapidement.[140]

Timing of Notification

Setting time limits on the notification by an organization to an administrative agency or a customer after a data breach seeks to balance the organization's wish to determine the facts of, contain and possibly take counter-measures (including contacting law enforcement) regarding the breach with the customer's need for timely information to take basic steps such as closing accounts or monitoring credit reports.

Most U.S. state laws require notification, as noted, directly to the customer, rather than to an administrative intermediary. Most state laws require that this notification be done in a very timely manner, with most simply requiring it be done as soon as is expedient. A typical example is Illinois:

> The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.[141]

This provision is clear that after basic steps to determine what is lost and to restore system integrity, customers should be notified without delay. Illinois does, however, have a delay for customer notification where a written request by law enforcement is made to the organization:

> The notification required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.[142]

Nonetheless notice must be made as soon as possible once notification "will no longer interfere with the investigation". Florida, Ohio and Wisconsin all require that at the limit, notification must in any case be made within 45 days of the determination of the breach.

[140] Transcript Montreal Group 1, at p. 52.
[141] 815 ILCS 530/10(a).
[142] 815 ILCS 530/10(b-5).

Therefore, in the U.S., notification is usually made in a very timely manner, ensuring that notices get to actual consumers quite quickly.

Administrative Notification

Canada's tendency to interpose an administrative notification stage prior to customer notification complicates the timing of the notices. Alberta's approach tends to follow that of the U.S., however, the timing of notices under Bill C-12 and the federal guidelines are more obscure, to the point of interfering with timely notice to customers.

Under Bill C-12

Bill C-12, the timing of notification to the Privacy Commissioner is specified in subs. 10.1(3).[143] It states that: "The report . . . must be made . . . as soon as feasible after the organization determines that a material breach of its security safeguards has occurred." While this test appears to require reporting "as soon as feasible", it does not so require. In fact, all that is required is that the organization report "as soon as feasible" once it has determined there has been a "material breach". Recall that determination of this materiality requires the organization in part to perform "an assessment . . . that the cause of the breach or pattern of breaches indicates a systemic problem." Thus the timing of the report is either: a) never, if the organization concludes there is no system issue; or, b) whenever the organization is able to conduct its "systemic problem" assessment and concludes that there is indeed such a thing. Yet "[t]he devil is in the details of how one implements such a thing",[144] that is, an assessment of whether an issue is "systemic" is not standardized. It could vary greatly between organizations and presumably could take a fairly lengthy time to perform if numerous systems were reviewed and at a detailed level.

Federally - Guidelines

There is no administrative requirement to report to the OPCC a data breach under the voluntary data breach guidelines. Therefore, there is no advice on timing, *per se*. However, the Guidelines offer this advice: "Organizations are also encouraged to inform the appropriate privacy commissioner(s) of material privacy breaches so they are aware of the breach." Presumably this is done in tandem with, or only slightly before, notifying individuals.

Alberta

Contrast this approach with Alberta's, which requires notice to the Alberta Commissioner to be made when there is a "real risk of significant harm to an individual" "without unreasonable delay".[145] The Commissioner then determines if notification of customers should take place under subs. 37.1 of PIPA. A continuing issue is whether an organization can take the position

[143] Bill C-12, s. 10.1(1) simply states an organization "shall report to the Commissioner any material breach".
[144] See comments of Dave McMahon, *infra*, at p. .
[145] PIPA, s. 34.1(1).

that in its own assessment "a reasonable person" would believe there was no "real risk of significant harm" and therefore it chose not to report.

Focus group members from Calgary appeared uncomfortable with this possibility, and stated it would be preferable to have all breaches reported, with the Privacy Commissioner alone making this determination, since the Privacy Commissioner would be reviewing the company's opinion in any case in all reported breaches where the company's opinion was that there should be no customer reporting.

> R: Yeah, like why is the company given the green light to decide whether to report it or not?
>
> M: So they should really notify the AIPC of everything.
>
> R: Absolutely everything, that's why they're in place. Then they have some teeth.[146]
>
> . . .
>
> M: Do you think the whole idea of having a database of data breaches … like, if all data breaches were reported to the Privacy Commissioner, does it also serve a purpose that it's also a good way of just tracking the whole phenomenon of data breaches so you know how many of them are happening every year and that this is a growing or a shrinking problem?
>
> R: I think it's a good idea. You can recognise patterns and ways to prevent, what to look for in future as far as their levels of advancement.[147]

Customer Notification

Under Bill C-12

The customer notification section in Bill C-12, s. 10.2, states in subs. 5 that:

> (5) The notification must be given as soon as feasible after the organization confirms that the breach has occurred and concludes that it is required to give the notification under subsection (1).

Thus administrative notification is a prerequisite to customer notification. While this approach is clear from C-12's proposed notification structure, it leaves the distinct possibility that the organization's initial investigation and determination of whether it should report to the OPCC

[146] Transcript Calgary Group 1 at p. 67.
[147] Transcript Calgary Group 2 at p. 37.

could be extended while assessing its "systemic problem". Although subsequent notification to customers (provided the breach further "creates a real risk of significant harm to the individual") should be "as soon as feasible", the initial scope for delay of the first stage seems at best naïve compared to the emphasis on timely disclosure required of U.S. organizations.

Another oddity with Bill C-12's timing requirement for customer notification is that there is no requirement to hold a notification if so requested by law enforcement. Presumably there are situations, such as a sting-type operation on a "rogue employee" who has stolen a database and seeks to market it,[148] where it would make sense to have such notification held. Yet, technically, withholding the notice while assisting law enforcement in this manner would be a violation of the C-12 amendments.

Federally - Guidelines

Under the federal breach notification guidelines, as noted above, the organization is first called upon to evaluate the utility of reporting the breach. Assuming it determines it should, the Guidelines offer the following advice on timing:

> **When to notify:** Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

Thus under the present guidelines, the approach is roughly that of most U.S. state legislation. This is in part because the Guidelines do not really contemplate an essential role for the OPCC, meaning notification to customers is really the relevant issue. However, it is clear that provided an organization decides to notify voluntarily, that customers actually are better off under the Guidelines' timing advice than under the Bill C-12 timing requirement.

Also, the Guidelines do contemplate holding notification while law enforcement is recommending withholding notice, in order to protect an investigation. Arguably, law enforcement is better off under the Guidelines than under Bill C-12.

Alberta

Timing of customer notification is coincident, as noted above, with administrative notice to the Alberta Privacy Commissioner. Where this is not the case is where the organization takes the view that although the data breach has happened there is no real risk of significant harm, it is possible that no notification by the organization to the Alberta Privacy Commissioner will result. However, it appears most organizations are erring on the side of reporting. This is likely due to

[148] This precise situation was described by Mr. Dave McMahon in stakeholder interviews. See *infra*.

two reasons. First, subs. 34.1(1) posits an objective test for "real risk of significant harm". Thus the harm is not in the eye of the breaching organization. Second, there is a specific penalty in PIPA for not reporting to the Commissioner when there is an objective "real risk of significant harm".[149]

With this background, we now turn to actual customer notice under the Alberta PIPA. Provided a report is indeed made to the Alberta Privacy Commissioner, the Commissioner in turn decides if he needs to order notification, if the organization has not already undertaken the notification already. This customer notification system via the Alberta Privacy Commissioner is found in subs. 37.1:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and
>
> (b) within a time period determined by the Commissioner.
>
> (2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).
>
> (3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of signification harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.
>
> (4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization
>
> (a) to notify individuals under subsection (1), or
>
> (b) to satisfy terms and conditions under subsection (2).
>
> (5) An organization must comply with a requirement
>
> (a) to provide additional information under subsection (4),

[149] " It is an offence not to notify the Commissioner of a security breach that poses a real risk of significant harm to individuals (section 59(1)(e.1)).": Alberta IPC, "Notification of a Security Breach - Personal Information Protection Act Information Sheet 11", at page

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

The requirements in this section provide the Alberta IPC a wide scope of powers to assist with ordering customer notification. The section also allows customer notification by the organization without Commissioner approval.

Notable is the requirement that the Alberta Privacy Commissioner "establish an expedited process" for those breaches "where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate". This power should assist with timely notification to customers in situations such as theft of credit card or banking information, where timely customer action is often crucial. However, despite some situations that would appear to be of this type,[150] it appears the Alberta IPC has not used an expedited process.

Source of Notification (Responsibility to Notify)

The issue of which party is responsible to notify customers is usually straightforward. It is usually the organization actually suffering the breach. However, parties often subcontract personal information handling tasks (see McMahon interview) and in these cases, and in others where there are payments system intermediaries or other agents, it can seem unclear which party has primary or ultimate responsibility to notify customers of breaches. It is also unclear whether one or both parties are required to notify.

Bill C-12

Under Bill C-12, this issue is not completely addressed. It is true that new subs. 10.1(1) requires an organization to report "any material breach of security safeguards involving personal information under its control", however, that control is not further defined as either

[150] For example, in *Aviscar*, discussed *infra*, where credit card details were deliberately skimmed at a third-party operator location of Avis.

contractual, agency-based or "de facto". However, PIPEDA has a general principle that both parties are responsible for personal information handling when it is subcontracted, with the original data collector primarily responsible for personal information handling.[151] It is perhaps assumed that this rule will apply in situations of data breach under the new bill, and the primary organization will notify, or that the (for example) subcontractor could notify if this is more appropriate.

Interestingly, the focus group members thought that it would be most prudent to have a rule requiring that the primary organization (the contractor not the subcontractor; or the principal, not the agent) be required to report. They believed this would promote a better understanding of the situation by customers. They gave examples of major retailers or banks that would be more appropriate notifiers than their payments' system providers:

> M: And also, who should the notice come [from]? Should it come from the company that you dealt with? In some cases that company might have sub-contracted their data processing to another company and they may be the ones who committed the data breach. So, if you get a notification should it be from the company you dealt with or should it be from the company that they may have …
>
> R: It should be the company you dealt with.
>
> R: M'hmm. [Yes.]
>
> R: Because you don't really have direct association with the other company or even know about that company.
>
> R: That they exist.
>
> R: Exactly.
>
> R: And giving more information to them than you thought you were.
>
> M: So, that would just raise more suspicion.
>
> R: M'hmm.[152] [Yes.]

[151] See PIPEDA, Sch. 1, Principle 4.1.3, which reads: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."
[152] Calgary Focus Group, 8:00 p.m., at pp. 40-41.

Again, a consumer-centric approach would put the duty on the party that the customer reasonably thought they were dealing with and with whom they have a commercial relationship. It would also help to dispel part of the fear and distrust around the breach.

It is quite conceivable that companies may wish to "pass the buck" on such notifications to a subcontractor. Reputational damage is cited by most companies as a huge concern - so having notice come from a subcontractor may be tempting.

We note that in our focus groups, however, we did ask participants if receiving a notice from a trusted company would lower their reputation with the customer or cause the customer to take his or her business elsewhere.[153] For the most part, the focus group participants stated they would not hold the company in lower esteem based on one breach, provided it was openly discussed in the notice and the personal information lost was not too sensitive. They only expressed likelihood to move their account if they were not assisted adequately with the breach, were notified of repeated breaches or if the information lost was egregious and jeopardized their financial security.

> M: If you did get a notice of a data breach from a company that you deal with, if they took the initiative to tell you about a data breach of some kind, how would it affect your relationship with the company, if at all?
>
> R: It depends on how they handle it when you talk to them. If they aren't really going to be very helpful about it or give any suggestions or send you to the right people to get things straightened out then you're not going to want to stay with them.
>
> R: But you have to respect their honesty.
>
> R: Yeah, for catching it and letting you know.
>
> R: We all make mistakes.
>
> M: Would you immediately take your business elsewhere or would you give the company a second chance if they notified you there's been a data breach?
>
> R: It depends, what Jo said.
>
> R: And everybody deserves a second chance but it depends on what it is, too.

[153] See also the section below, "Cost of a Data Breach" and the discussion in the Ponemon report of the costs of "customer churn".

R: And can you take it somewhere off?

R: Yeah, it could be a monopoly of some kind.

R: If it's your SIN it's pretty hard to get another one.

R: Exactly, I'm going to take that to the next company.

M: Well, the reason I asked that question is because I know that some companies have argued against having to notify the public about data breaches because they say, if we notify people, people will lose confidence in us and we would lose business. Other people say, if everybody had to notify, it would be a level playing field because every single company would be notifying so it would make everybody …

R: We'd all lose confidence in everybody.

M: We'd all lose confidence in everybody equally. But the point is, you have to bank somewhere.

R: But there's got to be a line drawn where they're worried about their own back pocket and they're more concerned about ours, because we're lining it. They need to have respect for us and letting us know about situations like that.[154]

The lesson appears to be that consumers will be wary of the situation with an organization after a breach, but that honesty and helpfulness will convince most customers to stay with the organization, provided there was not a loss of information like a SIN, which could cause severe financial losses.

Under the Guidelines

Under the federal data breach guidelines a similar approach to that preferred by the focus groups participants is suggested:

> **Who should notify:** Typically, the organization that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach by a retail merchant of credit card information,

[154] Calgary Focus Group 2, at pp. 41-42.

> the credit card issuer may be involved in providing the notice since the merchant may not have the necessary contact information.

While the emphasis on "the organization that has a direct relationship with the customer, client or employee should notify the affected individuals" is consistent, it appears, with consumer expectations, the qualification at the end of the paragraph creates some uncertainty and could lead to an organization taking the position that is was not responsible merely because the transaction was paid for with a credit card. This was a position that was taken by an organization under the Alberta PIPA as described below.

Alberta

Alberta PIPA specifies that an organization "having personal information under its control". In the *Aviscar* decision,[155] the Alberta IPC was faced with the argument from Avis that because car rentals were paid for by credit card, and Avis had no way to know if the credit cards were in fact being used fraudulently (but credit card "retailers" did), that the breach notification should come from the credit card "retailers" (Avis did not specify if this referred to the issuing bank or the credit card company itself). The Alberta Privacy Commissioner rejected this attempt to "pass the buck". He noted Avis' position was contrary to the policy of PIPA, which was to notify customers of a breach so that they can take steps to prevent harm or to mitigate it:

> [16] I reject Aviscar's submission that it would be most appropriate for the credit card "retailers", as opposed to Aviscar, to advise the affected individuals of this breach. The incident happened to Aviscar, not the credit card "retailers". PIPA requires the organization having the personal information under its control and which experienced the incident to report the incident and where I determine notification is necessary, to notify the affected individuals. In this case Aviscar is the organization that had the personal information under its control and experienced the incident, not the credit card "retailers". <u>The purpose of notification is to enable individuals to take steps as quickly as possible to avoid or mitigate the possible harm that may arise from the incident. Aviscar's suggestion that it should not be the party to have to notify because it does not know if the customer's credit card has been fraudulently used is not relevant. Whether the customer's credit card has been fraudulently used yet is not the point. The point is to inform the customer of the potential it may be used so the customer can take any steps he or she deems necessary to prevent fraudulent use.</u> Aviscar must notify the affected individuals and provide them with the details of the incident as required by the Regulation.

[155] Aviscar Inc., P2011-ND-001, January 6, 2011, Case File #P1739. Online: http://www.oipc.ab.ca/pages/OIP/BreachNotificationDecisions.aspx?id=3480

While the Alberta IPC found in this manner and likely in line with consumer expectations and the policy of the Act, it is tempting to wonder whether Aviscar relied to any extent on its own interpretation of the federal data breach guidelines in making the argument it was not responsible, or whether it simply tried to rely on the credit card companies' more developed systems to deal with customer fraud.

U.S. State Laws

It is worth noting that in the U.S., state laws generally have "third-party notice" requirements, which state that, if the subcontractor dealing with personal information is not the data's "owner" or "licensee", that third party must notify the primary party without delay, and, in some states, cooperate with the primary party towards notifying. Nevertheless, the notification must be done by, and is the responsibility of the "first" or primary party. A particularly good example of this language is found in the Massachusetts data breach statute.[156] However, Massachusetts further specifies that if, for example, a retailer were only handling "swipe data" from a credit card, provided other personal information was not kept at the retailer, that the retailer would not "have actual custody or control over the personal information".[157]

---

[156] Mass. Gen. Laws 93H § 3(a):

> Section 3. (a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

[157] See: Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00" (November 3, 2009). Online: http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf:

> **Except for swiping credit cards, I do not retain or store any of the personal information of my customers. What is my obligation with respect to 201 CMR 17.00?** If you use swipe technology only, and you do not have actual custody or control over the personal information, then you would not own or license personal information with respect to that data, as long as you batch out such data in accordance with the Payment Card Industry (PCI) standards. However, if you have employees, see the previous question.

Given the potential confusion and various possibilities for which entity could be considered to have "personal information under its control," it may be preferable for a Canadian federal data breach law, or regulations, to specify at this level who is responsible for data breach notification, in particular when dealing with payment transactions.

Method of Notification

The actual method used by the organization to notify customers can also have an effect upon the utility of such notices to consumers. Ideally, the notices should be delivered quickly to customers, but also reflect in their form the gravity of their content; that is, there is a risk that the notice will be simply treated as marketing material or not read as simply being unimportant.

California law was the first to tackle this problem. It allows for electronic notice (e-mail) to customers, but only if the customer has previously agreed to receive such notices electronically.[158] California law otherwise requires written notice, unless the breach is very large, in which case, "substitute notice" is permitted. This has been copied in most state laws:

> Most states have developed a substitute notice regime to handle large security breaches. In California, substitute notice can be used if the cost to provide written or electronic notice exceeds $250,000 or if more than 500,000 consumers are impacted. Substitute notice requires (1) email notice if an email address is on file, (2) conspicuous posting on the entity's website, and (3) notification of major state-wide media. Substitute notice by email does not require advance consent from the consumer – it is merely a good faith attempt at providing email notification. Under Delaware law, substitute notice can be used if the cost of the primary forms of notification exceeds $75,000 or if the number of affected consumers exceeds 100,000. At the other end of the spectrum, Maine applies $5,000 or 1,000 consumers as its threshold for substitute notice.[159]

Bill C-12 effectively adopts this approach, albeit leaving the finer details again to regulations (which are not yet published) in new subs. 10.2(6) which reads:

> (6) The notification must be conspicuous and given directly to the individual in the prescribed form and manner, except in the prescribed circumstances where it is not feasible to do so, in which case it must be given indirectly in the prescribed form and manner.

[158] California Civil Code, s. 1798.29(g)(2), 1798.82(g)(2) and 15 U.S.C. § 7001.
[159] CIPPIC White Paper, *supra*, at pp. 16-17 [footnotes omitted].

It appears substitute notice will be defined for certain breaches involving a number of records. Likely this will include a threshold number, a good faith effort to contact the customer by direct means, and include an element of public notice via the media.[160]

Returning to the default direct notice requirement, it will be interesting to see if the word "conspicuous" in this subsection is interpreted to require that notices are flagged in a standard, yet attention-getting way. It is interesting to examine the notices in Figures 1 and 2 above; note that there appears to be a risk that logo-heavy e-mails could be mistaken by the customer for marketing materials and deleted. In addition, there is the concern that many phishing e-mails have similar subject lines to our two examples.

Our focus group participants were concerned with confusion of such e-mails with spam and marketing, but also liked the convenience and rapidity of an e-mail notice:

> M: Now, tell me, let's say hypothetically that you were notified of a data breach. Like let's say for you C., your bank had a data breach and they notified you of it, what form should it take and what would you want to know?
>
> R: I'd want to know what was breached and …
>
> M: You mean like what information?
>
> R: Yeah. And, if they got a hold of financial information, what they're going to do about it so that none of my accounts can be withdrawn from or changed.
>
> M: T., what would you want them to tell you?
>
> R: Yeah, I'd want to know what it was. It would be sufficient enough to receive an email about it, as a form of communication. I don't need to be phoned about it.
>
> M: Or get a letter in the mail?
>
> R: Letter in the mail would work as well. But that may be an option to save on paper.
>
> [. . .]
>
> M: So like what the consequences could be?

[160] See P. Schwartz and E. Janger, "Notification of Data Security Breaches", Michigan Law Review, Vol. 105, p. 913 (March 2007) at 936, who note this is a form a "reputational sanction." Available online at SSRN: http://ssrn.com/abstract=908709

R: M'hmm. [Yes.]

R: I was going to actually more respond to the format that I would like it. And you had mentioned email, which is efficient, except for …

M: It might end up in your spam folder.

R: It could end up there, and also if it's someone that I don't know I would quite often delete. Because Hotmail all of a sudden will say if you don't do blah, blah, blah, your account will be … I just delete those. And so you might be tempted to delete it. Same with a phone call, I wouldn't want them to call me on my supper hour and tell me. I think I would want a letter. It would feel more official to get a letter. I would more likely pay attention to it.

R: A more personal contact.

R: Yeah.[161]

Given these potential pitfalls with e-mail notice, it may still be preferable for the regulations under Bill C-12 to express a method of preferring a hard copy letter notice, or telephonic notice in very serious situations likely to involve imminent fraud. Certainly the focus group participants appeared to expect that a data breach, especially one involving sensitive data or one likely to cause harm, would be serious enough to merit a hard copy form of notice, or, at the extreme, a faster notice:

> M. J'ai entendu ça aussi. Mais dites-moi autant que vous sachiez, lorsqu'il y a une violation de données comme par exemple dans une institution financière, au gouvernement ou dans un magasin de détail ou quoi, que doit-il arriver, comme quelle obligation à l'institution si tant qu'elle en ait? Comme si moi je suis la banque ou le gouvernement ou n'importe qui si moi je suis l'institution qui a les données ou qui a laissé une fuite ou qui a laissé traîné, c'est quoi mon obligation?
>
> R : Une fois qu'on le sait.
>
> R : Mais il faut savoir de où elle vient la fuite, elle peut venir de plein de places.
>
> R : Mais l'institution est tenue de nous aviser.
>
> R : D'envoyer une lettre à toutes ls personnes.[162]

[161] Transcript Calgary Group 1 at pp. 46-7.
[162] Montreal Focus Group 1 at p. 21.

. . .

> R. [. . .] Maybe what they need to look at is notifying everybody but doing it at, shall we say, different stages or different levels. If it's a "relatively insignificant breach", like a name was slipped but there was no other personal information, you can send them a letter. But if there was something of any serious consequence, then maybe you need to step it up and contact these people relatively quickly.[163]

Finally, it appears safer from a consumer perspective to have organizations attempt to reach them via various methods to try to ensure the message is received. On this point, wise advice comes from the federal voluntary data breach guidelines of the Office of the Privacy Commissioner of Canada, which states:

> **How to notify:** The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known. Using multiple methods of notification in certain cases may be appropriate. You should also consider whether the method of notification might increase the risk of harm (e.g., by alerting the person who stole the laptop of the value of the information on the computer).[164]

Encryption

One interesting consideration in a data breach regime is whether legislation should stipulate whether encrypted data should be exempted from the reporting or notification regime. For example, California state law requires notification only for breaches of unencrypted personal information.[165] The exclusion of encrypted data from the data breach regime would encourage companies to implement better data security practices that will likely prevent future data breaches. This has been advocated by some private organizations:

> Microsoft believes that encrypted information should be excluded. Data encrypted using standard methods is either impossible or impracticable to decipher. Therefore, there is no reasonable possibility of its misuse if it is accessed without authorization. In addition, by specifically exempting such encrypted information from the standard for notification, Congress will be creating an explicit incentive for companies to adopt encryption technology, thereby

[163] Calgary Focus Group 1 at p. 25.
[164] OPCC, "Key Steps", *supra*.
[165] California Civil Code at §1798.82(a).

> reducing the risk of a security breach in the first instance. If Congress has concerns that a general encryption exception is too vague and could be abused, Microsoft would support allowing the exception to apply only to certain levels of encryption —– e.g., the encryption level set forth in the Federal Information Processing Standards issued by the National Institute of Standards and Technology —– or more generally to encryption adopted by an established standard setting body combined with an appropriate key management mechanism to protect the confidentiality and integrity of associated cryptographic keys in storage or in transit.[166]

Massachusetts is a notable example of state legislation that not only requires encryption but also stipulates the minimum encryption standard expected for data. Massachusetts defines "breach of security" as:

> ... the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information ... that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.[167]

As noted above, our focus group participants were skeptical of a flat exemption from data breach rules for "encrypted" information. Their response indicates that a more detailed definition of what encryption is required and what level of exemption is attained from the duty to notify should be carefully considered.

Massachusetts thus considers encryption of data to be a good security practice, but does not provide a unilateral exemption for encrypted data as other state statutes do. The law is much more nuanced, and requires reporting of breaches where the process or key that is capable or compromising the security of encrypted data has been accessed or where the access of encrypted data creates a substantial risk of identity theft or fraud. Further, “encrypted” is defined as the "transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation." The department of consumer affairs and business regulation can adopt regulations to revise the definition of "encrypted" to reflect applicable technological advancements.

Encryption is particularly important to secure data stored on mobile devices, such as laptops and hard drives, that may be lost in transit. Therefore it is a policy question to decide if an exemption for "encryption" should be designed to provide a basic level of protection on these frequently lost or stolen storage media or if a higher level requirement should apply to assure near complete data security.

---

[166] Michael Hintze, Microsoft, Testimony Before U.S. House Subcommittee on Commerce, Trade and Consumer Protection, “Data Security: The Discussion Draft of Data Security Legislation” (28 July 2005).

[167] Massachusetts General Laws, Part 1, Title XV, Chapter 93H, "Security Breaches" at s. 1(a).

Enforcement of Notification Duties

Given that the decision to report a data breach largely depends on the interpretation of the notification thresholds in legislation, one important consideration that will weigh heavily on organizations is what enforcement measures are in place for the failure to report a data breach.

Bill C-12

The OPCC's current powers are limited to investigations of complaints filed by individuals and audits. The OPCC can investigate a complaint filed by an individual or initiated by the OPCC that addresses a contravention of the protection of personal information as set out in Division 1 of PIPEDA or the failure to follow a recommendation of Schedule 1 of PIPEDA.[168] The Commissioner is required to prepare a report that contains the Commissioner's findings and recommendations and any settlement that was reached by the parties.[169] Under the current ombudsman model, the OPCC's recommendations can only be enforced if the complainant or the OPCC applies to the Federal Court for a hearing.[170] The Federal Court may order an organization to correct its practices, order an organization to publish a notice of any action taken, and award damages to the complainant, including damages for any humiliation that the complainant has suffered.[171]

The question of OPCC enforcement powers under PIPEDA is a topic of ongoing discussion, in which Privacy Commissioner Jennifer Stoddart has vocalized the need for enforcement powers.[172] Commissioner Stoddart noted in a recent speech that Canada is one of the few major countries where a privacy regulator lacks the ability to issue orders and impose fines, stating that "[t]he privacy world has changed - and our laws need to keep up."[173] The nature and breadth of powers the OPCC needs is a much broader discussion than this paper allows, so the following discussion is restricted to the enforcement of the proposed breach of security safeguard provisions introduced in Bill C-12.

Bill C-12 does not come with strong enforcement powers for failing to report a breach to the Privacy Commissioner or for failing to notify individuals. Instead, the breach of security safeguards provisions are accompanied only a by slight expansion of the current complaints-based model.

---

[168] PIPEDA at s. 11(1).
[169] PIPEDA at s. 13(1).
[170] PIPEDA at ss. 14(1) and 15.
[171] PIPEDA at s. 16.
[172] Commissioner Stoddart stated in speeches that she would be raising the issue of enforcement power as part of the next mandated parliamentary review of PIPEDA, which was scheduled to take place in 2011. It is now clear that the parliamentary review of PIPEDA will not occur in the 2011 parliamentary calendar.
[173] Commissioner Jennifer Stoddart, "The Evolution of Privacy in an Online World" speech to the Women's Executive Network, Breakfast Series on 17 May 2011 in Ottawa.

Bill C-12 amends PIPEDA to give the Commissioner oversight over complaints related to the new breach notification requirements. This means that an individual could file a complaint to the OPCC if an organization failed to notify an individual of a breach where the breach meets the "real risk of significant harm" threshold.[174] However, this begs the question: how is a consumer to become aware that an organization has failed to notify them of a breach if the organization has not notified the consumer about a breach in the first place? Even if an individual otherwise becomes aware of a breach, he or she may not feel it is worth the time, effort and cost to pursue a matter even if it may be indicative of broader systemic problems within an organization. Relying on complaints to check for compliance with PIPEDA is ineffective and the Privacy Commissioner has noted: "At the moment, there is no simple mechanism for my Office to check compliance, unless we get a complaint. However, there are too many organizations collecting personal information for us to solely rely on a complaints-based system."[175]

Moreover, the complaints process itself has been characterized as "woefully ineffective" and "an exercise in futility" by Christopher Berzins based on his own experience with a complaint filed with the OPCC.[176] Notably, Berzins' complaint dealt with a data breach, so the facts pertaining to his complaint may be instructive. Berzins received a letter from National Bank notifying him of a data breach in the form of a stolen laptop. The letter informed him of the personal information stolen and assured him that "the computer was secure and the risk of fraud is limited". Berzins contacted the bank to find out whether the stolen information had been encrypted so he could make a more informed assessment of the risk. The bank would not provide any information about whether encryption was used and as such, Berzins filed a complaint under PIPEDA to the OPCC requesting confirmation of whether the stolen information had been encrypted. In his view, encryption of the data was essential to determine whether the information was properly safeguarded and the bank should be more transparent with its customers so they could make informed assessments of the risks they were exposed to and take appropriate actions to address the risks in a timely manner.[177] At the end of the

[174] Note that although an individual could file a complaint with the OPCC regarding security safeguards (PIPEDA, Principle 4.7) of the organization that may have led to the breach, it appears he or she cannot complain that the organization did not notify the OPCC of the breach at the administrative notice stage: See C-12, clause 13, amending PIPEDA, s. 14(1), which adds to the grounds for complaint: "as modified or clarified by Division 1 or 1.1, ... or s. 10.2". It is arguable that the "modification or clarification" of the safeguards principle is not adequate to ground an individual complaint that an organization did not first report to the OPCC; this is buttressed by the reference only to new s. 10.2 (customer notification), not s. 10.1 (notification to the OPCC).

[175] Commissioner Jennifer Stoddart, "The Evolution of Privacy in an Online World" speech to the Women's Executive Network, Breakfast Series on 17 May 2011 in Ottawa.

[176] Christopher Berzins, "Complaining under *PIPEDA:* An Exercise in Futility" Canadian Privacy Law Review Vol. 7, No. 9 (August 2010) at p. 106.

[177] Berzins' article "Complaining under *PIPEDA*: An Exercise in Futility" provides a more detailed overview of the facts of his complaint.

process, the OPCC determined that Berzins' complaint was well-founded, but failed to address the encryption issue.

Furthermore, the OPCC took approximately 16 months to complete the investigation in Berzins' case, which is not unusual. The OPCC 2010 Annual Report noted that the average complaint treatment time in 2010 was 15.6 months.[178] Notably, the average complaint treatment time for well-founded complaints was 21 months.

Notably, if the OPCC concludes that the complaint is well-founded and makes recommendations, these recommendations are only enforceable by a hearing at the Federal Court initiated by the individual. Bill C-12 amends PIPEDA so that the Federal Court can order an organization to comply with the customer notification provisions.[179] These procedural elements in the event of non-compliance with the notification requirements of Bill C-12 are time-consuming, so much so that by the time an investigation is resolved and the individual makes a successful application to the Federal Court, affected customers will have lost precious time to take precautions to protect themselves against malicious uses of the stolen data. This process is likely to be too frustrating for an individual complainant and will discourage all but the most determined complainants.

Under s. 11(2) of PIPEDA, the OPCC can initiate a complaint and investigation for the contravention of the breach of security safeguards provisions. However, it is important to note that the OPCC can only initiate a complaint if there are "reasonable grounds to investigate". It is unlikely that the OPCC would have reasonable grounds to initiate an investigation unless they have been tipped off by a whistleblower.[180] An important limitation of Commissioner-initiated complaints is that the Commissioner cannot apply to the Federal Court for a hearing.[181] This means that if the OPCC initiates an investigation into a security safeguards breach on the basis of a whistleblower tip, the OPCC is unable to apply to Federal Court to enforce their recommendations.

One notable omission from Bill C-12 is the extension of the Privacy Commissioner's powers to audit organizations to ensure compliance with the new Division 1.1 (Breaches of Security Safeguards) of PIPEDA.[182] The OPCC can only audit an organization if they have reasonable grounds to believe that the organization is contravening PIPEDA. Yet the OPCC has already

---

[178] *Office of the Privacy Commissioner Annual Report to Parliament 2010: Report on the Personal Information Protection and Electronic Documents Act* at p. 122. This is a decrease from 2009, where the average complaint treatment time was 18.5 months.

[179] Clause 14 of Bill C-12.

[180] Note that under clause 19 of Bill C-12, whistleblowers notifying the Commissioner of particulars with respect to a breach of security safeguards may request their identity to be kept confidential.

[181] PIPEDA at s. 15.

[182] PIPEDA at s. 18. Note Bill C-12 does not add "or 1.1" to this section.

found itself compelled to perform two major audits: in one case after repeated news reports of practices that had previously been the subject of a data breach complaint regarding resale of used computers,[183] and in the other upon the self-reported breaches of a number of mortgage brokers.[184] This is a major gap that potentially allows the underlying breach notification decisions to be unreviewable, unless and until a complaint is filed under the Safeguards principle in PIPEDA and even then an organization could question an audit of the actual notification decision, such as whether it actually did assess if the breach was evidence of a "systemic problem".

Thus, the breach of security safeguards provisions of Bill C-12 are not only disappointing because the thresholds leave too much room for interpretation that will likely lead organizations to decide not to report, but the glaring omission of any likely or meaningful penalty for failing to report a breach will mean that organizations are unlikely to report breaches to either the OPCC or to affected customers. Indeed, the Privacy Commissioner has called for "significant, attention-getting fines" on companies when poor privacy and security practices lead to breaches: "the only way to get some corporations to pay adequate attention to their privacy obligations is by introducing the potential for large fines that would serve as an incentive for compliance."[185] One possible mechanism of introducing "attention-getting" fines might be that of Administrative Monetary Penalties (AMPs), a civil penalty in which an administrative body or regulator seeks monetary relief against an individual or corporate body as restitution for unlawful activity. In the wake of the Commissioner's call for such "fining" power, the government of the day appeared open to considering this power.[186]

AMPs are imposed by the regulator without intervention by a court or tribunal and the regulator does not need to seek court approval of the AMP in order for it to be enforceable. AMPs can either arise automatically by operation of the law or at the discretion of the regulator. AMP schemes usually involve a notification procedure setting out the details of the violation and the financial penalty determined by the regulator to be applicable. An administrative hearing on the appropriateness of the penalty is generally set out in the governing legislation or regulation. Most administrative penalties provide for a right of review, although typically not before the penalty becomes enforceable. AMPs are especially popular in the field of consumer protection in Canada, such as for misleading representation and

[183] See OPCC, Audit Report of the Privacy Commissioner of Canada Staples Business Depot, Final Report. Online: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_staples_2011_e.pdf

[184] See OPCC, Audit of Selected Mortgage Brokers, Final Report. Online: http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_mb_2010_e.pdf

[185] Commissioner Jennifer Stoddart, "The Evolution of Privacy in an Online World" speech to the Women's Executive Network, Breakfast Series on 17 May 2011 in Ottawa.

[186] Sarah Schmidt, Postmedia News: "Clement open to large fines for massive data breaches — after further talk" (May 6, 2011). Online: http://ipolitics.ca/2011/05/06/clement-open-to-large-fines-for-massive-data-breaches-%E2%80%94-after-further-talk/ (accessed May 10, 2011).

deceptive marketing under the *Competition Act*,[187] telemarketing under the *Telecommunications Act*,[188] and the sending of unsolicited commercial electronic messages under the *Canadian Anti-Spam Legislation*.[189]

The time may also be right to introduce limited order-making powers for the OPCC with respect to breaches of security safeguards. In fact, order-making powers would enhance the profile and importance of privacy compliance officers as they would be responsible for avoiding sanctions, meaning that businesses would devote more resources to PIPEDA compliance and securing their systems against data breaches. The experience of provincial regulators has shown that the negative risks of order-making powers are seemingly overstated and would not likely erode the effectiveness of the OPCC's ombudsman model.[190]

Focus Groups Participants' Views of Enforcement Powers

All focus groups concurred that the privacy authority in charge of data breach notification should have a panoply of powers to ensure reporting to customers, including fines and order-making powers. Regarding fines, they noted that the fine for not reporting should exceed the savings of not notifying customers:

> M: Si une compagnie était victime d'une violation de données et ne l'a pas signalée comme la loi obligerait que devrait-il arriver?
>
> R : Une amende.
>
> R : Sanction.
>
> R : Oui mais c'est touché ça encore parce que si l'amende est moins chère que ce que ça lui coûte pour tous nous aviser.
>
> M : Une grande amende.
>
> R : Il faut qu'elle soit big.[191]
>
> . . .

[187] *Competition Act*, R.S.C., 1985, c. C-34 at s. 74.1.
[188] *Telecommunications Act*, S.C. 1993, c. 38 at s. 72.01.
[189] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23 at s. 20.
[190] Frances Houle and Lorne Sossin, "Powers and Functions of the Ombudsman in the *Personal Information Protection and Electronic Documents Act*, An Effectiveness Study" (August 2010).
[191] Montreal Focus Group 1 at p. 60.

M: Right. Now if a company had a data breach and didn't report it when the law said that they had to, what should happen to them?

R: Fine.

R: Heavy penalty.

M: But what should the penalty be?

R: It depends on the breach.

R: I was actually wondering that question earlier, what happened if they didn't?

R: $100 per person that it affected.

R: Yeah, that's an idea.[192]

. . .

M: […] Si une compagnie était victime d'une violation de données et ne le signalait pas comme la loi qui l'obligerait, que devrait-il lui arriver?

R : Des amendes.

R : Sévères et exemplaires.

R : Des amendes de 100 000 $ surtout pour les banques, ils peuvent payer des grosses amendes avec tous les frais qu'ils nous chargent.[193]

Some focus group members in Montreal thought that customers should even receive a statutory amount for non-notification (that is, the equivalent of a statutory damages award):

M: Alors une amende, quoi d'autre, comment on doit punir?

R : Une compensation aux gens qu'elle a pas avisé par exemple même si c'est 5 $ par personne je pense que ça fait plus mal inaudible en passant vous me devez un 5 $.

M : Parce que si c'est 100 000 personnes, 5 $ fois…

R : Mais en tout cas trouver un équilibre qui fait que… trouver un avantage à aviser.

[192] Calgary Focus Group 1 at p. 52.
[193] Montreal Focus Group 2 at pp. 44-45.

. . .

M : Est-ce qu'Ils devraient être obligés de payer un dédommagement au client?

R : Sûrement.

R : Oui.[194]

Many comments focused on the need, whether a fine was given or another course like a class action started, that the information about the organization that did not report should be made public, in other words, there should be a power of publication in the privacy commissioner, even to the point of allowing the privacy commissioner to notify affected individuals:

M: Je pense que D. a parlé d'une amende, est-ce que ce serait une bonne idée?

R : Moi je dirais pas que ce soit une amende, mais que ce soit dit publiquement, dans les médias, que ça sorte dans les médias, ça leur ferait plus mal, un coup à leur puiblicité, à leur réputation fait plus mal qu'une amende parce que souvent une amende ils vont s'en sortir.

R : Ou peut-être même les deux.

R : Ou les deux, mais il faut que ça faisse mal à leur réputation.

M: Passible d'action collective?

R : Passible d'action collective, il faut qu'on le sache pour ça si on le sait pas donc il faut que ce soit médiatisé.

R : Mais c'est vrai que dès qu'on se rend en cours va falloir que les vistimes dépensent de l'argent pour faire une action collective et il y a très peu de chances…[195]

. . .

R: I think the government at that point, if they're not listening and not telling people then I think the government should step in and say, okay, you know what? We're going to do it for you. And you need someone there, if the

[194] Montreal Focus Group 2 at p. 45.
[195] Montreal Focus Group 1 at p. 61.

company is not going to tell the people then you need something in place so somehow, some way, the people are told about it.

M: And that could be more embarrassing to the company if, instead of them notifying, it's …

R: Yeah. It's got nothing to do with the government, an outside body is not going to give a damn.

R: So they can do more damage that way than anything else. If I owned a big company I'd sure be thinking twice, because I wouldn't' want that happening to my company.

R: That's a very good point.

Focus Group participants also considered audits of the information practices and reporting practices of the organizations could help with reducing data breaches and increasing reporting:

M : Ou peut-être avoir un audit de ces pratiques de sécurité.

R : Sur une liste de surveillance par la même instance qui fait la législation.

R : Il faut que ça attaque leur réputation en tout cas.[196]

. . .

M: Now, what about could you have a situation where maybe they would have to be audited for their security practices by the Privacy Commissioner if they were caught not notifying?

R: I think seriously any company should turn around and welcome that and say, hey, take a look and see if we're doing anything wrong, or is there anything we can be doing better? It's almost like getting a certification. You can turn around and tell your public, hey, we're checked every year and we're doing good.[197]

Alberta

Contrast the proposed enforcement of the breach of security safeguards provisions in Bill C-12 with the Alberta approach in *PIPA*, which states that it is offence to fail to notify the

[196] Montreal Focus Group 1 at p. 61.
[197] Calgary Focus Group 1, at p. 53.

Commissioner of a security breach that meets the harm threshold.[198] A person who commits an offence is liable to a fine of up to $10,000 if they are an individual or a fine of up to $100,000 if they are a person other than an individual (e.g. a corporation). Thus, the Alberta data breach regime is accompanied with high fines for failure to report a breach. This potential for a large fine provides incentive for organizations to report the breach to the Privacy Commissioner.

As discussed above, the Commissioner can require an organization to notify individuals about a breach. *PIPA* states that organizations must comply with a Commissioner's requirement to notify individuals.[199] The Commissioner has already issued a number of breach notification decisions wherein his office requires organizations to notify individuals about a breach. The Commissioner's written decision to require an organization will be issued within 10 days of the OIPC having received all information required to make a decision and the Commissioner may publish any decision.[200] The Commissioner has exclusive jurisdiction to require an organization to notify individuals.[201] If an organization fails to notify individuals in accordance with a Commission decision, the Commissioner has the power to make an order and can file a copy of an order with the Court of Queen's Bench so that the order is enforceable as a judgment or order of that Court.[202] Furthermore, failing to comply with an order made by the Commissioner constitutes an offence under s. 59(1)(f) and the business could be liable to a fine of up to $100,000.

Enforcement for Breaches in Health Information Privacy

Many provinces have legislation governing the collection, use and disclosure of health information as well as individual access to their own health information. Provincial health privacy legislation usually applies to health information in the custody or control of "custodians". Under the Alberta *Health Information Act*, there is no requirement to report breaches to the Privacy Commissioner or to notify affected individuals about privacy breaches. However, the Alberta Privacy Commissioner reported that in 2010-2011, custodians' self-reported 43 privacy breaches and most custodians who self-report go on to voluntarily notify patients affected by the breach. The Commissioner notes that this high level of voluntary self-reporting and notification is "reflective of health services providers' professional obligations to protect patient confidentiality."[203] This professional obligation in the health sphere does not apply to private sector contracts between businesses and consumers, and thus private sector organizations cannot be relied upon to voluntarily report breaches to the Privacy Commissioner based on a duty of confidentiality to notify affected individuals.

---

[198] Alberta PIPA at s. 59(1)(3.1).
[199] PIPA at ss. 37.1(1) and 37.1(5)(b).
[200] PIPA at s. 38(6).
[201] PIPA at s. 37.1(6).
[202] PIPA at s. 36(1)(b) and s. 52(6).
[203] Office of the Information and Privacy Commissioner, "2010-11 Annual Report" at p. 13.

Private Right of Action

Where there is no private right of action explicitly allowed within a statute, consumers must rely on provincial consumer protection, false advertising, implied contract, and fraud laws to bring a lawsuit against a private company.

Only statutory tort right of action for breach of privacy exist in British Columbia, Manitoba, Saskatchewan, and Newfoundland. Currently, there is no statutory private right of action allowed under PIPEDA, meaning that a consumer's remedy for a breach of PIPEDA is to first file a complaint to the Office of the Privacy Commissioner and then enforce that complaint by filing an application for judicial review with the Federal Court. The Federal Court has broad authority to award damages to the complainant, including damages for any humiliation the complainant has suffered. However, the Federal Court has only awarded damages in the amount of $5,000 in one instance since the introduction of PIPEDA ten years ago. In addition, the Federal Court read-down their power to award damages by stating that damages only apply in the "most egregious of violations".[204]

These tools are vague, at best, and do not provide a framework that is adequate for dealing with data breaches. A private right of action puts enforcement in the hands of individuals, meaning that enforcement is not completely left to the state. In the context of data breaches, a private right of action can give an individual the right to sue an organization for failing to notify them of a data breach or delays notification regarding a data breach.

The proposed data breach provisions in Bill C-12 do not include the private right of action as a possible enforcement mechanism. Instead, individuals would need to rely on judicial review in the current model to seek damages, which may be difficult given the Federal Court's recent statement that only the most egregious of violations would warrant damages.

The Alberta *PIPA* allows a limited private right of action for violations of *PIPA*. Individuals have a cause of action against organizations where the Commissioner has made an order and the individual has suffered as a result of the breach.[205] Individuals also have a cause of action against persons who have been convicted of an offence under the Act.[206] However, in both cases, the cause of action is limited to damages for loss or injury that the individual has suffered as a result of the breach or conduct. This means that individuals in Alberta could sue private organizations who were convicted of an offence for failing to report a breach to the Privacy Commissioner or where the Commissioner ordered the organization to notify affected individuals of a breach. However, the action would be limited to proven damages for loss or

[204] *Randall v. Nubodys Fitness Centres*, 2010 FC 681.
[205] PIPA at s. 60(1).
[206] PIPA at s. 60(2).

injury that the individual suffered as a result of the failure to report or the breach or the breach itself.

In contrast, California's data breach law, which is recognized to be one of the strongest data breach laws in America, gives consumers a statutory private right of action for data breaches. Thus, if a business fails to notify individuals of a data breach, individuals can institute a civil suit against the business to recover damages.[207] Notably, many state statutes provide for attorney general enforcement. For example, Maine's data breach statute gives enforcement powers to the Attorney General, states that violation of the law is a civil violation that is subject to a fine of up to $500 per violation, up to a maximum of $2,500 for each day the person is in violation of the law.[208] Some statutes that give enforcement powers to the Attorney General are not clear whether the private right of action remains available to individuals. One such example is highlighted by the American Bar Association:

> [I]n states such as Arkansas, the law is unclear. Section 4-110-108 of the Arkansas Code states that any violation is punishable by action of the attorney general, but then it goes on to incorporate by reference Sections 4-88-101 through 4-88-115. Section 4-88-113(f) specifically provides for private rights of action. One could argue, therefore, that although the attorney general is given enforcement powers under the statute, the incorporation of Section 4-88-11(f) preserves the right of an injured individual to bring suit.[209]

There are challenges with using a private right of action to enforce data breaches. Data breaches often do not cause any identifiable or quantifiable harm to the individuals whose information was compromised.[210] There also may be difficulties proving causation. One report

---

[207] California Civil Code SB 1386, §1798.82. Note that under California law, the threshold for notification is "breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

[208] Maine Revised Statutes, Title 10, Part 3, Chapter 210-B, "Notice of Risk to Personal Data" at §1349.2.A.

[209] John P. Hutchins & Anne P. Caiola, *U.S. data breach notification law: state by state* (American Bar Association, Section of Science & Technology Law, 2007).

[210] Note that the ULCC recommended against a private right of action in their 2010 Report, *supra*. They stated:

> [28] Likewise the Uniform Act does not provide for statutory damages for the data breach or for the failure to notify according to the Act. It simply notes that the availability of a civil remedy - for the breach or for failure to notify - is not affected by the Act. It is acknowledged that the absence of statutory damages may make it difficult for people whose personal information has been compromised without notice to recover from the person who has had control of the information. Certainly the American experience has been that such suits have failed, most often for lack of proof of damages. However, the consistent inability to prove damages in such cases may be in large part due to the lack of actual damages. Arguably the legislature should not provide what the evidence does not justify. This conclusion is the stronger when one considers damages for failure to give notice, and not for the initial breach – which may or may not have resulted from a breach of the obligation to take reasonable care that personal information be secure.

noted that courts in the United States have labelled the damages claimed by plaintiffs in data breach lawsuits as "speculative" or "nonexistent" and have dismissed lawsuits because of this defect.[211] Despite these challenges, the existence of a statutory private right of action may be a useful tool to encourage initial reporting of the data breach to regulators and notifications to affected individuals.

In considering the usefulness of including the private right of action as part of a broader enforcement regime, one example is the recently passed Canadian Anti-Spam Law (CASL). For violations of the specific provisions of the Act prohibiting the sending of a commercial electronic message and installation of a computer program without consent, CASL combines the use of administrative monetary penalties (AMPs) by enforcement agencies with a statutory private right of action that stipulates statutory damages.[212] The statutory private right of action is constructed such that any person who alleges that they are affected by an act or omission that constitutes a contravention of certain provisions of CASL may apply to a court for an order against an offending party.[213] Furthermore, CASL gives the court the ability to order the offending party to compensate the individual for actual loss or damage suffered or expenses incurred, or to pay statutory damages. The statutory damages vary according to the contravened provision, but generally allow a maximum award of $200 for each contravention not exceeding $1,000,000 for each day on which a contravention occurred.[214] The private right of action is not available if the offending party has entered into an undertaking or has been served with a notice of violation. Where the party has been served with a notice of violation, the party would only be subject to an AMP if the enforcement agency deems the penalty appropriate. Under CASL, the private right of action coupled with statutory damages serves as strong incentive for private organizations to ensure that they are compliant with the Act, and where they are non-compliant, to enter into an undertaking with the enforcement agency immediately. This should result in strong compliance with CASL.

Where underreporting is a common trend for data breaches because it is in the private organization's best interests not to report, strong enforcement mechanisms are needed to encourage reporting. Perhaps the inclusion of a statutory private right of action with statutory

[211] Gregory T. Parks & Megan E. Adams, "Can Your Firm Be Sued for a Data Breach?" E -Commerce Times (12 August 2006).
[212] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23, "Canadian Anti-Spam Law" or "CASL". Section 20 sets out administrative monetary penalties, factors that must be taken into account when determining the quantum of the AMP and allowing a maximum penalty for a violation of up to $1,000,000 for an individual and $10,000,000 for any other person.
[213] See CASL at s. 47(1).
[214] CASL at s. 51(1)(b).

damages for failing to report a data breach could serve as strong incentive to report. This could further promote compliance if the private right of action becomes limited or unavailable when the party reports a breach to the OPCC and provides notice to affected customers. Businesses would then likely be encouraged to immediately report breaches to the OPCC and notify affected customers so as to minimize their liability.

U.S. Data Breach Laws and New Developments

Forty-six American states, as well as the District of Columbia, the Virgin Islands, and Puerto Rico, now have enacted data breach laws. The four states that still have not are Alabama, Kentucky, New Mexico, and South Dakota.

U.S. law firm Perkins Coie has a comprehensive PDF summary of the key points of each state's legislation.[215] There also is a summary of State Security Breach Notification Laws from the National Conference of State Legislatures.[216] This chart also links to the legislation in the District of Columbia, the Virgin Islands, and Puerto Rico (the Perkins Coie resource does not contain these references).

Most U.S. state legislation is still based on the pioneering California S.B. 1386 legislation.

Massachusetts recently has created a regulation to its security breach legislation that requires all businesses and other entities dealing with Massachusetts residents to create a comprehensive written (but reasonably tailored to the size of the entity) security plan for dealing with personal information.[217]

Recently, several federal data breach bills have been proposed;[218] most would pre-empt state laws in this sphere. One bill would require reporting of all data breaches to the Federal Trade Commission within 48 hours; the FTC could then fine organizations that did not so report.[219] In addition, the White House has released a draft Cybersecurity Legislative Proposal, which will cover "sensitive personally identifiable information". Some U.S. consumer groups have worried

[215] Online: http://www.perkinscoie.com/statebreachchart/
[216] Online: http://www.ncsl.org/default.aspx?tabid=13489
[217] Referred to as "201 CMR 17.00", this general security requirement law appears to be the "next generation" of security laws, requiring as it does that entities take prior action to achieve a standard level of data security. It includes a section on "Duty to Protect and Standards for Protecting Personal Information" and one on "Computer System Security Requirements". The law has been controversial and its implementation was delayed for some time until 1 March 2010 to ready businesses. Online: http://www.box.com/shared/static/4k3kh7v4bt.pdf
[218] George V. Hulme, "They're baaack! National data breach notification bills resurface," CSO Magazine, June 27, 2011, online: http://www.csoonline.com/article/685125/they-re-baaack-national-data-breach-notification-bills-resurface provides links to the bills, none of which yet appears to have gained enough support for passage.
[219] See: http://bono.house.gov/UploadedFiles/Data_Breach_Draft.pdf

out loud that protections on certain information in the California state law will be weakened by these moves.[220]

Data breach notification requirements under European Law

What are the current rules regarding data breach notification under European Law?

With entry into force of the amendments to the ePrivacy Directive (2009/136/EC), telecom operators and internet service providers in the European Union are now required to notify a competent national authority of any personal data breaches without undue delay.[221] In addition to this requirement, the applicable legal threshold to notifying an individual is if a breach is "likely to adversely affect the personal data or privacy" of the subscriber or individual in question. In these circumstances, a service provider has an additional requirement to promptly notify this person or persons.[222] Exception to this last obligation is made however, if the provider can demonstrate, to the satisfaction of the competent authority, that they have implemented appropriate technological protection measures and that these measures have been applied to the data in question.[223] This amendment expands on article 4 of the Directive on privacy and electronic commerce 2002/58/EC that simply articulated a general requirement for communication service providers to inform subscribers of a particular risk of a breach and any remedies and costs that may be involved.[224]

---

[220] Center for Democracy & Technology, WH Cybersecurity Proposal: Good Start on Data Breach Notification (may 25, 2011). Online: http://cdt.org/blogs/cdt/wh-cybersecurity-proposal-good-start-data-breach-notification

[221] Europa News Release/Communiqué MEMO/11/320 "Digital Agenda: how new EU rules improve privacy protection for internet users" (23 May, 2011) online: <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/320&format=HTML&aged=0&language=EN>

See also:

DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws online: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF> [ePrivacy Directive 2009/136/EC] at article 2 4) (c) 3; Europa News Release/Communiqué IP/11/887 "Digital Agenda: Commission consults on practical rules for notifying personal data breaches online" (14 July, 2011) online: < http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/887&format=HTML&aged=0&language=EN&guiLanguage=en>; and ENISA *Data Breach Notification in the EU* (13 January, 2011) online: < http://www.enisa.europa.eu/act/it/library/deliverables/dbn>

[222] ePrivacy Directive 2009/136/EC at article 2 4) 3.

[223] ePrivacy Directive 2009/136/EC at article 2 4) 3.

[224] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) online: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF> [ePrivacy Directive (2002/58/EC)]

The amended article 4(3) further adds that after having considered the possible adverse effects of a breach, a competent national authority may require a provider to notify the subscribers or individuals concerned if the provider has not already done so. This section also provides minimal standards for the content of any notification issued to both a consumer and to a national authority.

Article 4(4) grants extensive powers to competent national authorities, including; issuing guidelines and instructions regarding the circumstances in which providers are required to notify about personal data breaches, the format of such notifications as well as the manner in which such notification is to be made. Under 4(4) competent national authorities are also able to conduct audits to determine if providers have complied with their notification obligations and impose appropriate sanctions on companies that have failed to do so. Lastly, article 4(4) places an obligation on providers to maintain an inventory of personal data breaches that include the facts surrounding the breach and the remedial action taken, to allow competent national authorities to verify compliance with paragraph 3.

Finally article 4(5) grants the Commission the authority to adopt technical implementation measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in the article. The Commission has recently engaged in consultations to assist in the implementation of such measures.[225]

2) What are the European Union's plans to extend these notification requirements to other industries?

In its *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, the Article 29 Data Protection Working Party stated that policy development was expected in the context of extending the personal data breach framework of the ePrivacy Directive to the context of the general review of Directive 95/46.[226] Such developments are in accordance with the Commissions commitment before the European Parliament to initiate consultations with stakeholders with a view to presenting

[225]Europa ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications Public consultation (Consultation Document) online: http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/data_breach/ePrivacy_databreach_consultation.pdf

[226] Article 29 Data Protection Working Party 00683/11/EN WP 184 <http://idpc.gov.mt/dbfile.aspx/WP_184.pdf.> at para 4. The declaration was made in the context of the reform of the Regulatory Framework for Electronic Communications < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN> [00683/11/EN WP] This commitment was also reaffirmed in Communication from the commission to the European Parliament, the council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>

proposals on the subject by the end of 2011.[227] In its document, the Working Party also states that the Commission should rely on the same or very similar core elements, such as the definition and threshold to notify data subjects, as the one used in the ePrivacy directive, as it would be counterproductive to apply different criteria to other data controllers than to providers of electronic services.[228]

Finally, it is important to note that recital 59 of the eDirective encourages Member States to adopt the notification requirements to all sectors, stating that the "interest of users in being notified is clearly not limited to the electronic communication services." Despite this explicit recommendation however, most Members, with the exception of Germany and Austria, have not yet done so.[229]

Statistics – How much breaching are Canadian organizations really doing?

Unfortunately, good statistics on data breaches from Canada are limited. We have only a short experience, in Alberta, with mandatory notification of consumer-oriented breaches (with Ontario's Health Information Privacy Act, we have information on health-related breaches). Given the amount of discretion provided to organizations to report under the proposed federal legislation (Bill C-12) there may not be more Canadian information of note even if the bill passes (at least in its present form).

The findings of the TELUS-Rotman joint study on Canadian IT Security Practices as well as annual reports of four of the five private sector privacy commissioners do, however, provide some clues as to the prevalence of data breaches in Canada.

In the U.S., the Identity Theft Resource Centre attempts to keep a detailed listing of data breach statistics. These sources are detailed below.

We can, however, compare U.S. numbers under state laws with Canada. The trend overall there is up, so seeing numbers go down in the OPCC Annual Report is curious.

---

[227] *Ibid*. See also: Viviane Reding "Assuring data protection in the age of the internet" (SPEECH/11/452 Presented to the BBA (British Banker's Association) Data Protection and Privacy Conference, 20 June, 2011) online: < http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/452&format=HTML&aged=0&language=EN&guiLanguage=en > at p. 3

[228] 00683/11/EN WP at para 33-34. It should be noted however that in her speech to the BBA, Viviane Reding stated that the applicable threshold to notify for the banking industry would be a "serious data breach". It remains to be seen how this will be interpreted. See also paragraph 39 of the Working Paper that warns against tailoring sector specific technical measures implemented under the act.

[229] 00683/11/EN WP at para 11 and 18.

Canadian Statistics

In the private sector, few reports have gathered data on either security breaches or data breaches and recorded them in a comprehensive manner. Some of these reports are: the *TELUS-Rotman joint study on Canadian IT Security Practices* (TELUS-Rotman), the Federal Office of the Privacy Commissioner of Canada's *Annual Report to Parliament on the PIPEDA*, the Office of the Information and Privacy Commissioner of Alberta's *Annual Report* and the Office of the Information and Privacy Commissioner for British Columbia's *Annual Report*. In addition, the OPCC commissioned a study on the attitudes of Canadian businesses to security breaches and the possibility of data breach legislation. The findings of each report are discussed below.

The TELUS-Rotman Joint Study on Canadian IT Security Practices

TELUS and the Rotman School of Management, University of Toronto have, since 2008, conducted joint annual studies on the state of IT security in Canada. More than 600 IT security professionals responded to the 2011 study "allowing TELUS and Rotman to provide clarity on the Canadian security landscape, especially as it relates to emerging trends in breaches, threats and preparedness."[230] Of particular interest for the current report, the Joint study asserts that numbers of "security breaches" in all sectors have been on the rise since 2008. More specifically, in 2011, there was an annual average of 7.6 security breaches per respondent in the public (meaning public corporations, as opposed to government), private (meaning private corporations) and government spheres. That is, each organization averaged 7.6 "security breaches" a year.[231]

Although there seems to be a decrease in the number of security breaches in the private corporation sector, the joint study indicated that this may be attributed to "reduced investment in detective technologies by private organizations due to the economic slowdown; they may be less targeted by attackers, or less inclined to report a breach even if they detected one."[232] Meanwhile, for public corporations, "Public organizations have surpassed government agencies in the annual number of breaches for the first time since the beginning of the study (18 breaches for public companies against 17.3 for government organizations)."[233] The report notes that, for government and public organizations "[b]oth sectors are affected by compliance legislation, including privacy and credit card security standards. These regulations mandate the

---

[230] Telus – Rotman Joint Study on Canadian IT Security Practices 2011 Intro page. Online at: http://promo.telus.com/manage_risk/2011/survey/. Full Report online: <http://business.telus.com/en_CA/content/pdf/whyTELUS/Security_Thought_Leadership/TELUS_Rotman_2011_Results.pdf>

[231] The question asked to the security professionals was "33. How many security breaches do you estimate your organization has experienced in the past 12 months?" See TELUS-Rotman Study 2011, at p. 31.

[232] *Ibid.*, at p. 6.

[233] *Ibid.*

deployment of detective technologies, which increase visibility into potential data breaches (and allow for their remediation). With increased visibility comes increased reporting."[234]

What is crucial to understand regarding the TELUS-Rotman Report is that "security breaches" are not necessarily also "data breaches".[235] In addition, "security breaches" need not be reported under any Canadian legislation, unless personal information also is breached.

The overall impression left by the TELUS-Rotman Report is, however, that security breaches - that can certainly lead to data breaches depending on the motivation of the attacker or other factors - are very common. Indeed, one would expect that such a large number of security breaches would leave the distinct possibility that in some minority of these cases, there would be a data breach that would meet the Alberta data breach reporting standard.

Office of the Privacy Commissioner of Canada

Data breaches, and data breach reporting, are discussed at section 4.8 of the Federal Privacy Commissioner's most recent Annual Report to Parliament (2010). The Commissioner begins this section by reminding readers that the Privacy office encourages organizations to voluntarily report data.[236] A telling indicator of the success of such non-binding requests is revealed in the statistics for 2008-2010. During this time period the number of data breach incidents voluntarily reported to the Commissioner declined two consecutive years in a row, from 65 to 48.[237] The OPCC states it is looking forward to data breach legislation and notes that:

> A mandatory reporting scheme will give us a clearer picture of how many breaches are occurring, why they are occurring, and what steps should be undertaken to reduce the risk of future incidents.[238]

Unfortunately, under the administrative notification regime in the legislation referred to by the OPCC (then Bill C-29, now Bill C-12), given the degree of discretion allowed to organizations to self-assess if a breach is "material" and the addition into this test of a self-assessment of

---

[234] *Ibid.*, at pp. 5-6.
[235] See Interview with Jacob Glick, Counsel, Google, who makes this distinction.
[236] Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2010 - Report on the Personal Information Protection and Electronic Documents Act* (June 2011). Online: http://www.priv.gc.ca/information/ar/201011/2010_pipeda_e.pdf at p. 85 [OPCC Report to Parliament 2010]
[237] OPCC Report to Parliament 2010, at p. 85. It should be noted that the financial industry appears to be routinely reporting breach incidents. In 2010, two-thirds to voluntary breach reports came from financial institutions. While the OPCC praises this as transparency, this may indicate simply that this sector has the most breaches, in part due to the amount of sensitive (financial and other) data they hold relative to other sectors. However, this may also be related to class action lawsuits that have been filed against financial institutions for data breaches.
[238] OPCC Annual Report to Parliament 2010, at p. 85.

"systemic problems" it is unclear how much clearer the picture will be even after this legislation is passed.

Alberta

In its 2011 annual report, the Information and Privacy Commissioner of Alberta affirms that since breach notification became a mandatory in May 2010, the Office of the Information and Privacy Commissioner of Alberta (OIPC) had received 97 breach notifications and now is processing on average 8 breach reports per month.[239]

After the introduction of the mandatory data breach notification law, private sector data breach reports jumped from 15 to 49, increasing more than threefold.[240]

As noted in the section on customer notification under Alberta's PIPA above, in 17 of these 49 reporting cases, the organization resisted customer notification and had to be ordered to so notify. It is unclear from the Alberta IPC Annual Report how many of the remaining 32 data breach reports to the Alberta IPC resulted in customers being notified (as the company can choose to voluntarily report directly to customers) and in how many the Alberta IPC confirmed that no customer notification was necessary. Without transparency regarding this final number, and perhaps recitation of some illustrative cases, it is fair for consumers to question how many data breaches are not being reported, and why.

It also seems reasonable to question whether many data breaches which would satisfy at least the Alberta standard for disclosure are taking place across the country but are not being reported to the OPCC, not to other privacy commissioners, nor to consumers.

British Columbia

The statistics available for British Columbia's privacy regimes are based entirely upon self-reported breaches and those in which the Office of the Privacy Commissioner of B.C. has issued a "public interest notification". The Office of the Information and Privacy Commissioner for British Columbia's 2010/2011 Annual Report provides data related to breach notification for both B.C. FIPPA and PIPA, however the information is not segregated by Act, meaning public and private data breach reports are mixed. There were 71 self-reported breaches under both Acts in 2009-2010 and 64 in 2010-2011.[241] There were 12 "public interest" notifications (of data breaches) in 2009-2010 and 16 in 2010-2011.[242]

---

[239] Office of the Information and Privacy Commissioner of Alberta *Annual Report 2010-11* (October 2011) online: < http://www.oipc.ab.ca/Content_Files/Files/AnnualReports/AR_2010_2011.pdf> at p 6 32-34 (Table 1 and Graph 1)

[240] *Ibid.*, at p. 15. Note that the Alberta IPC refers to these as "self-reported" breaches. It appears that when an organization reports to the Alberta IPC a data breach, it is recorded as "self-reported" even if the organization felt compelled to report by the PIPA.

[241] Office of the Information and Privacy Commissioner for British Columbia 2010-2011 Annual Report p. 14 online: <http://www.oipc.bc.ca/publications/annual_reports/OIPC_AR_2010_11.pdf> The report states the following

Ontario

Finally, in Ontario, there are mandatory reporting requirements in the *Personal Health Information Protection Act* for individuals' personal health information. According to the most recent *Personal Health Protection Act (PHIPA) Report*, there were 96 self-reported breaches made in 2010 and 101 in 2009.[243]

United States

Data breach statistics in the United-States are much more robust, if still fragmented. For example, for the year 2011 (to date in November 2011) according to the data breach statistics published by the Identity Theft Resource Centre (ITRC), 375 data breaches had already occurred, compromising some 26,000,000 records.[244] In 2010, ITRC reported 662 breaches that compromised over 16,000,000 records.[245] The ITRC numbers are lower than other U.S. data breach estimates, as the ITRC defines a "data breach" as when "an individual name plus Social Security Number (SSN), driver's license number, medical record or a financial record/credit/debit card is potentially put at risk."[246] The number therefore also includes medical data breaches. In addition, the ITRC data is compiled only from credible public sources, that is, it is not based on any particular reporting requirement.[247]

Finally, according to Verizon's 2011 *Data Breach Investigations Report*, a total of 761 data breaches were said to have occurred compromising 3.8 million records in the U.S. in 2010.[248] Ironically, on page 47 of the report Verizon notes that the number of records compromised in

---

regarding public bodies/organizations: Public bodies and private organizations frequently ask us for advice on privacy or access implications of proposed policies or current issues. They may also ask us to review privacy impact assessments they have prepared for proposed policies or programs.

[242] Section 25 of FIPPA requires public bodies to disclose certain information in the public interest and to notify the Commissioner. It is also worth noting that at p. 8 of the Annual Report the privacy commissioner stated the following: "In the case of private sector privacy regulation, the number of organizations governed by PIPA is so large and the potential consequences of privacy breaches so severe that mandatory reporting of privacy breaches to my office and to consumers should become a legal requirement, as it is under Alberta's equivalent law."

[243] Information and Privacy Commissioner of Ontario *Personal Health Information Act (PHIPA) Report* online: < http://www.ipc.on.ca/site_documents/ar-10-e-PHIPA.pdf> at p.5

[244] Identity Theft Resource Centre *2011 Data Breach Stats* online: <http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202011.pdf>

[245] Identity Theft Resource Centre *2010 Data Breach Stats* online http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202010.pdf

[246] *Ibid.*, at p. 11.

[247] *Ibid.*, at p. 11: "Each item must be previously published by a credible source, such as Attorney General's website, TV, radio, press, etc. The item will not be included at all if ITRC is not certain that the source is real and credible."

[248] Verizon's 2011 *Data Breach Investigations Report* online: <http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf> at p. 11. These breaches were all those that been confirmed as either Verizon, or the U.S. Secret Service, had been called in to assist with investigation of the data breach. It therefore only represents a subset of total U.S. breaches. See pp. 7-8.

2010, was significantly lower than in previous years (in 2008, 360,834,871 records were compromised and in 2009, that number was 143,643,022) leaving the authors without a clear explanation for the significant drop. Leading hypotheses of the authors were high profile prosecutions of certain criminals accused of being involved in data breach operations. However, the Report notes: "The 2010 dataset has more breaches than ever before, but fewer compromised records."[249]

Thus, leading statistics in the United States tell a tale of somewhere in the high hundreds and perhaps thousands of reported and unreported data breaches. Despite the somewhat fragmented statistics on data breaches that are currently emerging from the United States, they appear to indicate the problem is underreported in Canada under the present voluntary federal guidelines. If nothing else, Canada's current data breach regime needs to be adjusted to facilitate the collection of data for the production of better statistics so that consumers, policymakers, privacy commissioners and security professionals would be better equipped to determine how data breaches and subsequent notification should be addressed depending on the size of an issue, an economic sector, and other trends in the misappropriation of data. In addition to these last benefits, more substantive statistics on data breaches would facilitate further academic research on the subject as well as allow for an easier comparison between Canadian data breach statistics and those in the United States, our most comparable and linked society.

Costs of a Data Breach

The cost of a data breach to an organization that suffers one is likely to parallel generally accepted costs borne from the experience of other companies – that are now considered to be upwards of $200 per individual record breached.

The Ponemon Institute's "The 2010 Annual Study: U.S. Cost of a Data Breach" Report

The study explores data breach experiences of 51 U.S. companies from 15 different industry sectors. [250] The Ponemon Institute used benchmark analysis, whose unit of analysis is an organization.[251] The Institute conducted in-person and telephone interviews with individuals within those organizations. The breach size analyzed by the Institute ranged from approximately 4,200 to 105,000 lost or stolen records.

---

[249] *Ibid.*, at p. 48.
[250] The Ponemon Institute, "2010 Annual Study: U.S. Cost of a Data Breach" online: http://msisac.cisecurity.org/resources/reports/documents/symantec_ponemon_data_breach_costs_report2010.pdf , p. 3.
[251] *Ibid.*

According to the Ponemon study: "Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from last year."[252] It is important to note that the Ponemon study attempts to include costs of lost business to other direct costs of responding to a breach and notifying customers. In relation to costs of lost business, Ponemon noted:

> The cost of lost business stayed relatively stable at around $4.5 million for the third straight year. In that time, lost business has decreased proportionally to overall data breach costs; in 2010, it accounted for 63 percent of the total cost, down 3 percent from 2009 and 6 percent from 2008. The decrease in spending on lost business closely matches the amount spent on detection and escalation and ex-post response.[253]

Ponemon explained, "abnormal churn or turnover of customers after data breaches appears to be the dominant factor in data breach cost. Regulatory compliance contributes to lower churn rates by boosting customer confidence in organizations' IT security practices."[254]

Ponemon attributed this shift in spending to a shift in focus at U.S. organizations from "data breach mitigation" to "regulatory compliance" and concluded: "Compliance with data protection regulations requires organizations to do more to find, disclose and fix breach-related problems."[255]

The Institute's more granular findings were that more U.S. organizations are opting in favour of rapid response to data breaches and that this stance is costing them significantly. Specifically, the study showed that "quick responders had a per-record cost of $ 268", which was up from $ 219 (22%) from the year before.[256] The results are suggestive of the point that initial high costs may be especially incurred during the detection, escalation, and notification phases.[257] Among a myriad of data breaches, those that constitute malicious or criminal attacks increased the most in 2010 while negligence remains the most common threat to data protection and is increasingly expensive ($ 196 per record).[258]

---

[252] *Ibid.*, at p. 5.
[253] *Ibid.*
[254] *Ibid.*, at p. 6.
[255] *Ibid.*, at p. 5.
[256] *Ibid.* p. 4.
[257] *Ibid*.
[258] *Ibid*. p. 6.

Finally, the Ponemon study noted that an organization experiencing a data breach for the first time incurred higher costs than those that had already responded to a breach.[259]

The 2011 TELUS-Rotman's "Joint Study on Canadian IT Security Practices"

As noted above in the statistics section of this report, the *2011 TELUS-Rotman "Joint Study on Canadian IT Security Practices"* on security breaches in Canada is based on responses of 649 organizations (government, public, and private) to a 52-question survey.[260] The survey findings indicate that costs associated with dealing with security breaches for all three types of organizations declined in 2011 from the previous three years. Specifically, in 2011, the average cost for all three types of organizations was $ 82,903 compared to $ 179,508 in 2010, $ 834,149 in 2009, and $ 423,469 in 2008.[261] The report states that this data may suggest that protection technologies have improved. However, the report also warns that:

> these reduced costs should not lure organizations into a false sense of security… As [the reports'] results continue to show, attacks are increasingly focused, with hackers targeting information that can be monetized or used for political and ideological gains.[262]

Unauthorized access to information by employees in all three types of organizations was found to be the most common type of security breach.[263]

The TELUS-Rotman report on Canada's IT Security Practices is helpful for a sense of overall corporate security spending, but it analyzes costs associated with dealing with *security* breaches as opposed to dealing specifically with *data* breaches as was analyzed by the Ponemon Institute. In other words, costs attributable to dealing with security breaches may include dealing with data breaches but they also include many other IT costs of dealing with security breaches, and may not include the costs of notifying the public where corporate data, not personal information, was the subject of a breach. Therefore, there is a need for a study conducted in Canada similar to the Ponemon report that shows how much it costs to deal with data breach per individual record.

---

[259] *Ibid.*, at pp. 5-6: ""first timers" paid the highest average costs of anyone in the 2010 study. This year, the cost per compromised record of an organization's first data breach averaged $326 (up $98 or 43 percent). These findings may indicate that attacks are becoming more insidious and damaging, which would require greater resources to combat. First timers often lack breach response experience that can help lower costs."

[260] TELUS-Rotman, "2011 Joint Study on Canadian IT Security Practices" online: http://business.telus.com/en_CA/content/pdf/whyTELUS/Security_Thought_Leadership/TELUS_Rotman_2011_Results.pdf, p.3.

[261] The study specifies that in 2011, it cost $ 195, 588 for public organizations to deal with security breaches, $ 70, 833 for private organizations and, $ 58, 929 for government organizations. See more on p. 12.

[262] *Ibid*.

[263] *Ibid*. p. 8

The lessons from Ponemon's study, and to a lesser extent the TELUS-Rotman study, are that it is expensive to suffer a breach and it costs more to deal with it quickly and if it is the organization's first data breach.[264] Also, regulatory compliance helps reduce lost customers and lowers the cost (and perhaps the chance) of data breaches. This indicates that a regulatory solution that includes incentives to avoid data breaches in the first place may be the most cost-effective. It also explains the relative resistance of organizations to report unless required to (costs and churn) and perhaps some of their reluctance to act quickly.

Stakeholder Interviews

PIAC also undertook stakeholder interviews to provide industry perspective as well as context and personal insight to the research. In particular, PIAC approached those persons who had written about data breaches, worked in IT departments dealing with data breaches, or who were active participants in the initial consultations by the Office of the Privacy Commissioner of Canada to develop the first data breach notification Guidelines. References to these interviews are also made in footnotes where the stakeholders agree or disagree with a statement made or position taken in the rest of this report.

Jacob Glick, Google

Mr. Jacob Glick, Google's Canada Policy Counsel, brought a unique corporate perspective. He first outlined some of Google's services. There are several Google services in which users may chose to store sensitive data, including Gmail, Google's webmail product, however, not all elements of GMail communications were sensitive.

Mr. Glick's noted that security breaches are not necessarily the same as data breach.

He recounted that at Google in 2010, certain human rights activists' Gmail accounts were targeted by attackers. This had nothing to do with Google or the integrity of its systems because the attacks focused on compromising the passwords of the targeted users.

Mr. Glick noted (correctly, based on the Alberta IPC reports of data breaches) that many data breaches, as opposed to security breaches, would be the result of unencrypted personal information being stored on local media. In his opinion, in the present age of encryption and

[264] Note that Ponemon and Symantec sponsor an online tool that is meant to assist organizations in calculating the potential costs of a data breach. See http://DataBreachCalculator.com

cloud computing, keeping such unencrypted data on local storage was much less safe than using “cloud” based services.

Mr. Glick's opinion of Bill C-29 (at the time) was that it would provide "zero consumer protection". Regarding the "systemic problem" requirement in the bill, he noted that this realization likely only would become obvious post-investigation and reporting.

Mr. Glick noted with data breaches it may sometimes be difficult to identify whom to notify. In addition, sometimes the content of what should be in the notification is not clear. He noted that new s. 10.2 of the Bill might not provide enough flexibility (in timing) in complex breach situations.

Mr. Glick's final comments were aimed at providing a bill that was more responsive to consumers and more focused on redress and rehabilitation after a breach. He suggested that the law should be aimed at providing consumers a way of fixing real problems, if harm materializes after a data breach. For example, if a consumer’s identity is stolen and their credit is adversely affected, there should be a way for them to restore their rating with credit agencies.

David Elder, Stikeman Elliott

David Elder is a lawyer who practices communications, competition and privacy law in the Ottawa office of Stikeman Elliott, where he is a member of the Communications, Competition and Foreign Investment, Privacy & Data Protection, Government Relations, Regulatory and Public Policy practice groups. Mr. Elder was formerly Vice President, Regulatory Law with Bell Canada, where he also served as Bell Privacy Ombudsman, the equivalent of Chief Privacy Officer. He has also served as Legal Counsel to the CRTC.

Mr. Elder noted that, speaking only his own opinion and not that of clients or his firm, that he favours a breach notification regime that encourages reporting of breaches to the Office of the Privacy Commissioner of Canada.

Mr. Elder thought more could be done to improve data handling at many organizations. He was referred to the Massachusetts law requiring general corporate security standards when dealing with personal information and concurred that such requirements could be useful for defining a legal standard of negligence in Canadian law regarding handling of personal information.

Regarding the (then Bill C-29) customer reporting threshold of "real risk of significant harm", Mr. Elder wondered whether "significant harm" would be interpreted by the OPCC as actual

financial loss, or the "hassle of dealing with ID theft" or the amount of time a customer would have to spend to deal with the problem?

Digging more deeply, he noted that the new subs. 10.2(3) of (then) Bill C-29 listed the factors to be considered in assessing significant harm (sensitivity of the personal information and probability that it will be misused) but wondered if additional factors would help to clarify the issue, such as an additional requirement to consider the number of persons affected or a clear statement that financial loss, or simply lost time to take preventive steps, would be considered such harm.

David McMahon

Mr. McMahon's role is solving Complex Security Problems for a large corporation. His responsibilities include advanced security for business markets and government contracts, largely with “security-heavy” aspects. He is responsible for all aspects of client facing security solutions, including: technology, legal, pricing, strategic planning, business development and marketing.

When asked what he considered to be a “data breach,” Mr. McMahon first explained the structure of a typical company’s data holdings, including personal information holdings. Most have: 1. Corporate information holdings; 2. Customer information holdings; 3. Communications information holdings. He noted that the draft privacy law’s (Bill C-29 at the time) definition of “data breaches” is mostly centred in the second type of holdings (personal information databases such as customer profiles and accounts), with some in communications records and rarely in corporate records. Those that are in category 2 are data breaches in the sense of the legislation (C-29) and would definitely be reported if detected. Those under category 3 are either a) customers or b) other communications company customers – but both are composed of transmission of information over public/private networks. The element of these being communications records and the regulation of telecommunications by the CRTC puts these records in a somewhat grey area.

In response to a question of whether a "data breach" was in any way different from a “security breach”, Mr. McMahon noted that a security breach (hacking; exploits; malware/botnets – at user end) is one way to get at data; another is negligence or penetration of the company.

On the infected (end-user) side (whether a consumer or wholesale customer with traffic traversing managed networks) there is a real reticence on the part of home, corporate, private or public sector users to have their infected computers cleaned by the provider, even if it can

be demonstrated that the infection is transmitting their personal information. People seem to be unwilling to pay additional to their ISP to have the ISP secure their Internet connection or home computer, despite for example some ISPs offering premium upstream / cloud security services. The telecoms and internet service market is a commodity-based market with users only caring (seemingly) about price for similar stated bandwidth. He suggested the legal regime has not yet reflected this reality.

The market reality is that companies and consumers /customers do not want to pay for this level of security. There is no incentive to have detailed "metrics" of attacks, breaches, etc. reported.

As for internal breaches, he stated that these could happen in any organization. In cases of internal employee malfeasance, companies will want time to investigate this sort of situation and solve it without the complication of reporting. Furthermore, companies would welcome assistance from law enforcement and government in preventing attacks and prosecuting those responsible for the breach. In these cases he suggested a better approach would be to go after the criminals not the victim.

These answers raised the issue of internal audit trails for access to personal information held by a company. Mr. McMahon noted that most companies have such audit trails and these apply to all customer records (including call records) and can identify responsible employees. Companies generally undertake internal audits of personal information accesses; following up on breaches is often a matter of resources to do "forensics on yourself".

We also asked about non-reported breaches and why they were not reported within industry. Mr. McMahon thought that such breaches may take considerable time to investigate and the problem was often solved internally; that there were resource constraints on "digging deeply" to discover the whole problem, which may uncover in turn a larger problem. He noted that third (or 4th or 5th) party breaches (where information handling was subcontracted) were difficult to investigate. He stated that few organizations, including public sector, would dig hard for evidence of breaches if they know that they will be penalized when it is found.

We then asked what his overall assessment of the "experience" of a data breach was from a systems protection perspective. His main insight was that security, operations and business parts of larger organizations might not always have same incentives to investigate breaches.

We noted the Ponemon Institute in the U.S. has suggested that the cost to an organization of a data breach is about US $200 a record. We asked Mr. McMahon if this seemed accurate. He replied that it would first be required to define a "record" and how this was measured. In the abstract he thought it was very difficult to assess the accuracy of this statement.

We then noted the (2010) TELUS and Rotman School of Business Report, which said that the cost of detecting and remedying data breaches had dropped rapidly in 2009 (78%) and that it was likely due to better protection technology and better organization within organizations. Mr. McMahon noted that it did not appear that this report is not based on any empirical evidence. It is compiled by interviews of security staff and is primarily subjective or anecdotal. He thought that there is often a substantial perceptual gap between what people believe and reality. The TELUS/Rotman study also noted that there had been lately more "focused and targeted" intrusion attempts -- targeted and focused meaning the purpose of the breach was squarely to seek personal or corporate information. Mr. McMahon confirmed that there is a trend towards focused attacks, albeit automated ones.

We then asked what are the most frequent sources of breaches. For example:

- Lost (smart)phone
- Laptop
- USB key/harddrive
- CSR database
- Outside hacking
- Cloud computing
- Outsourcing

He noted the answer depends upon both the definition of a "data breach" or "security breach" and which of the breach types is involved (referring here to which type of data (the 3 categories above) is involved. His understanding was that the largest volume of data breaches is compromised personal computer accounts (due to remote control by "botnets"). Outsourcing may be another source.

We then asked if companies do any information technology outsourcing and if so, how does one ensure data breaches are reported to it by outsourcing providers. (We noted here: the TELUS/Rotman report stated there is no increase in data breaches attributable solely to outsourcing).

Mr. McMahon was of the opinion that the Rotman conclusion on this point is not convincing owing to evidence to the contrary. The TELUS report stated that there is a belief amongst those interviewed that there is no increase in data breaches attributable solely to outsourcing. He stated that all large companies outsource. Outsourcing is a business decision. Outsourcers are most often required by contract to follow data practices required by the parent company. The problem is verification, compliance and sub-sub delegation. Parent companies may have insufficient resources or authority to audit third parties including forensic audits to see if they do what they claim to or do what they claim not to do. It appears that brand protection does

not factor as heavily into the calculus of outsourcing as perhaps a security department would recommend. This factor cannot be alone relied upon to encourage such oversight.

Turning to a recent IT development, we asked if there were any new or unique issues arising from cloud computing technologies regarding data breaches and if security departments take any additional or special measures when using these resources to protect personal information (e.g. encryption or a higher/better/more complete level of it). Mr. McMahon noted that cloud computing can increase the likelihood of additional jurisdictional problems, control, data sovereignty and situational awareness if not engineered correctly. It can also solve many of these issues.

We drew Massachusetts' law requirements to Mr. McMahon's attention, including the fact this state requires all companies to follow general computer security measures regarding personal information management, including:

- Secure user authentication protocols
- Secure access control measures
- Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly
- Reasonable monitoring of system for any unauthorized use of or access to personal information
- Encryption for all personal information stored on laptops or portable devices
- Up-to-date firewall protection and operating system security patches
- Up-to-date versions of system security agent software malware protection, patches, and virus definitions
- Education and training of employees on proper use of the computer system and the importance of personal information security

We then asked if he had any comments these measures, whether they were likely to be effective and if mandating them would make personal information safer and at what cost.

He replied that mandating these approaches is not likely to be very effective against advanced persistent threats. Firstly, whatever makes it into legislation will be out of date by the time it must be implemented. Secondly, the description of actions is too general to be implemented by security professionals. He felt the only solution is a principles-based, technology-neutral requirement to achieve best practices regarding security. Another focus for the law should be "end client expectations", that is, would it be reasonable to the end client that personal information had been handled by multiple sub-contractors and does the client have a right to

have the data kept fairly close to the original company with which they did business? This is a reasonable person standard.

He also thought that there should be a trend towards real-time detection of threats that is encouraged by legislation or by best practices that are mandated. Ideally, notification (to end users and victims) should be in real-time if they have subscribed to such a service.

He believed that other legal incentives that may work are personal liability for executives [as exists for environmental spills] and making level of security an element of network performance that is counted in executive compensation [many executive pay arrangements in Internet or communications rely upon increasing volume, so there is no incentive to reducing traffic – even malicious traffic – by implementing security to make the network "cleaner"].

Ultimately, he felt legal incentives alone may be inadequate. There is presently an "acceptable level" of security maintained which is not industry best practice but is industry standard. Tier 1 [telecommunications] carriers are trying to "raise the bar" by publishing industry articles in security magazines on best practices,[265] etc. and in direct petitions to the government.

He thought that what should really work is a "business case" for better security. An example would be showing that security increases led directly to fewer help desk calls (which are very expensive to companies).

PIAC then noted that the new amendments to PIPEDA (Bill C-29; now C-12) will require companies to determine, when they have a data breach, if it is evidence of a "systemic problem" – if so, it may mean notifying the Privacy Commissioner of Canada. We asked if this is a useful standard and would he feel comfortable in determining this for the industry.

Mr. McMahon stated he would not feel comfortable determining this because "the devil is in the details of how one implements such a thing."

PIAC also noted the threshold for notifying individuals of a data breach in the new amendments to PIPEDA is whether the breach will create a "real risk of significant harm". We asked if this was a useful standard in relation to the way a company deals with data breaches? Again, Mr. McMahon stated it was too vague to be implemented.

We then noted that the new amendments (Bill C-29/C-12) list factors to consider in assessing if the breach creates a "real risk of significant harm", including (i) the sensitivity of the personal information; and, (ii) the probability that such personal information will be misused. Are these

[265] Mr. McMahon provided the following example article: David McMahon and Tyson Macaulay, Upstream Intelligence in the World of Legal Compliance and Liability, IAnewsletter Volume 13, No. 4, Fall 2010. Hosted at: http://www.bell.ca/web/enterprise/newsRoom/en/pdf/Upstream_Intelligence_World_of_Compliance.pdf?EINT=secgrc_en_txt_prd_emk

factors sufficient? Do they reflect the factors you consider in determining the severity of a data breach?

Mr. McMahon stated, "This is a good start."

We then asked about Alberta's breach notification law penalties for not reporting a breach and noted the PIPEDA amendments do not have penalties for non-compliance. We asked if it is appropriate to penalize a company financially or otherwise for not reporting a "reportable" data breach? Why?

Mr. McMahon felt that the Alberta approach was "like punishing the victim". He felt that the fines need to be on the persons who created the breach.

Mr. McMahon then volunteered some interesting thoughts on how to improve security and the problems that lead to a call for data breach legislation:

1. Possible solution: self-regulatory – create working groups of related companies. If organized by sector, that sector can work on security problems and compare results with other sectors of the economy. If one sector falls behind they can be made/shamed to improve security as that sector will be seen as effectively transferring security costs to another sector.

2. Possible "credit rating" of traffic from particular companies or users. How "trustworthy" is their traffic? You could get a "cyber-rating" like a credit rating. Could force improvements to security in affected businesses or sectors or even individuals. Example: ISP McColo in the U.S. that was shut down for repeated spam hosting.

Mr. McMahon's position as a security expert was very illuminating of the challenges of dealing with data breaches from the perspective of the organization suffering the breach. We have therefore provided his comments at some detail as his perspective provides insight on many of the issues involved in data breach legislation and the possible implementation challenges of such requirements.

Conclusion: A New Approach Needed

The "data breach problem" is a litmus test for modern consumer protection. The root of the problem is the clear conflict of individual privacy and data collection and handling methods of organizations. Personal information is the "new currency" of the digital economy - yet this currency is not yet adequately protected. Real harms, many financial such as ID theft, but also

reputational and emotional can result from carelessness or inadequate security procedures of organizations entrusted with that personal information.

Yet, for each individual, the capacity to know that their personal information has been accessed in an unauthorized manner is extremely limited. This knowledge is entirely within the organization holding the personal information. Likewise, the consumer's ability to know of the organization's information handling practices or general corporate security stance is virtually nil. Finally, any attempts to use the court system to vindicate consumer rights regularly are tripped up on the hurdles of proof that any harm suffered is linked to the breach or even that the harm is worthy of monetary damages.

Yet data breach notification is simply another form of consumer disclosure. Consumers need this information to judge with whom to entrust, and how to further protect, their personal information, yet this information is, in Canada outside Alberta, largely unavailable.

Based on PIAC's examination of data breaches and recent legislative responses to them in Canada and abroad, it is evidence that, from a customer viewpoint, Bill C-12 is seriously flawed and will lead to next to no reporting and no effective protection for consumers. These extensive flaws should be addressed in major amendments to the Bill.

Bill C-12 grants excessive discretion to organizations that have had a data breach to characterize the breach as non-harmful to consumers. In so doing, organizations gain the benefit of a largely unreviewable decision, made by themselves under trying circumstances, in the face of a manifest and undeniable conflict of interest.

Given the relatively high costs of mitigating data breaches, including negative publicity and possibility of customer churn, as well as the lack of enforcement powers in the Office of the Privacy Commissioner of Canada, nearly all incentives point organizations away from data breach notification.

Data on data breaches is missing in Canada; policymakers, legislators, consumers and corporate security experts are effectively operating in the dark. What little data there is appears to suggest data breaches are routine and routinely underreported and that corporate data security could be improved.

A new approach is needed. Incentives must be aligned to encourage reporting, which will support consumer protection, increase consumer confidence, increase corporate data security and avoid largely fruitless litigation over data breaches.[266]

[266] See Appendix 4 - PIAC Legal Memo on Data Breach Class Actions in Canada. In conclusion, it notes: "Although breach-related expenses have been considered in the determination of the benefits awarded in such agreements,

Recommendations

Based on our study, PIAC believes that there are certain key aspects to effective federal data breach legislation. These must be added as structural amendments to Bill C-12:

1. **There should be a duty to report <u>all</u> data breaches[267] to the relevant privacy commissioner, either "as soon as reasonably possible" or within a short time window such as 48 hours;**
2. **There should be clear monetary penalties for not reporting to the privacy commissioner;[268]**
3. **The privacy commissioner should decide on customer notification, based on a harm test. This test should be objective and based on the standard of "real risk of significant harm"[269];**
4. **The privacy commissioner should be given the power to order an organization to report a breach to customers. Orders to notify customers should be made public as should the name of the organization involved;**
5. **The privacy commissioner should have adequate audit powers to examine corporate data security practices and in particular to examine an organization's data breach notification preparedness and response;**
6. **The adequacy and effectiveness of the data breach regime should be separately evaluated at the time of the next review of PIPEDA or provincial privacy legislation.**

The following recommendations may not require legislative change, and should in any case be implemented whatever the legislative framework chosen.

---

the issue of damages, and what constitutes damage in data breach cases, has not been directly addressed by the courts and remains a barrier to a successful data breach class action suit. *Larose* c. *Banque Nationale du Canada* offers some insight as the Court states that the fear of identity theft or fraud does not constitute harm or injury in and of itself and cannot provide a basis for class actions."

[267] That is, there should be no initial test of harm in the duty to report breaches to the privacy commissioner and no other discretion in an organization not to report. The policy reason against reporting all breaches (notice fatigue on consumers) does not apply here, as the privacy commissioner will make a second customer notification decision based on the harm standard.

[268] These penalties should have an upper limit which can be used by the privacy commissioner to encourage reporting as a cheaper alternative to treating a data breach as just another cost of doing business.

[269] It appears that the standard of "real risk of substantial harm" has achieved some acceptance across governments and business and although it should be reviewed along with the legislation, is adequate for now for consumers if it will speed customer notification at the privacy commissioner stage. See also P. Schwartz and E. Janger, "Notification of Data Security Breaches", Michigan Law Review, Vol. 105, p. 913 (March 2007) at p. 967, which recommends a "likelihood of misuse" standard which is a high-level endorsement of this type of standard, in part to "reduce the danger of information overload", that is, consumers receiving so many notices they ignore them.

7. **The privacy commissioner should create a dedicated data breach division, with adequate staffing, to address only data breaches.**
8. **The privacy commissioner should convene a "data breach advisory board" to bring current corporate information security expertise, consumer protection expertise and government regulatory expertise to bear on the question of data breaches.**
9. **The privacy commissioner should take a lead role in informing Canadians of how breach notification works, including a dedicated web page and online resources.**

Additionally, Parliament (and legislatures) should closely consider the arguments for non-disclosure to customers when personal information is encrypted and what an adequate level of encryption might be. Also, Parliament (and legislatures) should consider arguments for and against a time-limited exception to customer notification if requested by law enforcement involved in an investigation.

Therefore PIAC supports an "Alberta model modified" data breach law at the federal level. This will ensure consistent consumer protection at an adequate level across the country.

The proposed changes will likely engender a large requirement for additional staff at the various privacy commissioners' offices. However, once a certain experience with breach notification is achieved and once levels of expected notifications are known, it is hoped that the costs will be manageable. Once costs of a data breach both for organizations and consumers have been better documented with real figures, a more serious assessment of the true cost of, and cost of not, having data breach notification can be made. Ideally, with high administrative reporting requirements and penalties for non-reporting, organizations will be led to invest in more robust data security. This should produce a virtuous circle of better security, fewer breaches and less reporting.

However, the five year review of the data breach regime could, with adequate figures to back it up, lead to questions of whether a more robust or different regime were needed. It appears, for example, that the new trend may be towards corporate security requirement legislation, as in Massachusetts. If this were to be the case and there was a demonstrated jump in effectiveness at reducing data breaches from such an approach, the Canadian data breach regime could be adjusted to any new security legislation or new data security parts of legislation added to PIPEDA and provincial privacy acts, at that time.

Appendix 1 - Focus Group Transcripts

[Please see attached document Appendix_1_Focus_Groups.zip]

Appendix 2 - Environics Report on Focus Groups

[Please see attached document: Appendix_2_Environics_Report.pdf]

Appendix 3 - PIAC's notes on the Panel, entitled "Anatomy of a Data Breach"

Anatomy of a Privacy Breach

Panellists:
Moderated by John Beardwood, Vice-Chair Privacy and Information Access Group, Co-Chair Technology and Intellectual Property Group, Fasken Martin DuMoulin LLP
Patricia Kosseim, General Counsel of the Office of the Privacy Commissioner of Canada
Jill Clayton, Assistant Information and Privacy Commissioner of Alberta (Private Sector Privacy), Calgary
Janice Campbell, Risk Manager and Privacy Officer, Department of Quality and Risk Management, Hospital for Sick Children, Toronto
Suzanne Morin, Assistant General Counsel, Regulatory Law & Policy and Bell Privacy Ombudsman, Bell Canada

1) Threshold for reporting to Commissioner (called "notify" in Alberta PIPA)
   - PIPEDA has more flexibility
     - Objective test with subjective assessment of company
     - Reporting is to fulfill 4 purposes
     - PIPEDA standard is similar to CBA proposal (see chart)
   - Alberta PIPA – threshold is significantly lower (# included) and significantly higher (low sensitivity with large #)
     - Objective test – inconsistent with Industry Canada?

2) Threshold to notify affected individuals
   - Alberta regulatory authority makes the call so there is no reasonable requirement?

3) Define "significant harm"
   - PIPEDA deems certain things to be significant
   - AB PIPA not defined – guidance more general than PIPEDA
   - John Beardwood thinks this should be in the guide, not in PIPEDA
   - "real risk" does not provide any real clarity

4) Responsibility for notification
   - CBA perspective is that Privacy Commissioner should not be the gatekeeper

5) Offences

Case Study #1: personal information in stolen car

A bank branch office in Waterloo, Ontario, loses two sets of confidential employee files. The first set has duplicate copies, so the bank knows the name of the employees in question (the "Known Employee Files"). The second set was of certain new and transferred employees and had not yet been copied, so bank does not know which specific individuals were identified in the files (the "Unknown Employee Files").

The files were in the car of an HR employee, which was stolen in Waterloo. The employee's recollection is that the hard copy files of the Known Employees were under the driver's seat, and that the laptop with the "Unknown Employees" was in the trunk. The files are not encrypted, but access to the laptop is password protected, albeit with a very simple, 6-digit password, which happens to be the same as the customized licence plate. The police believe that it is possible that a person with minimal IT experience could open the laptop.

Case Study #1 Additional Facts

The Known Employee Files contain relatively generic and non-sensitive information about the employees work records. However, one of the employee files references that the subject employee, who is a practicing Muslim, has requested and been granted access to a storage room for the purposes of periodic prayer throughout the day. At the request of the employee, both the request and the granting of such request, have been kept confidential. The Bank knows that this particular employee, for various reasons, would like to continue to keep such information confidential.

The Unknown Employee Files may or may not contain sensitive information.

Does the breach pass the material breach threshold to be reportable?

Case Study #1 Additional Facts
The stolen car was eventually recovered, two days later. There are no suspects, but the police suspect university student joyriders. The hard copy files of the Known Employee were still under the driver's seat. The laptop with the "Not yet Known Employees" files was still in the trunk, but suffered damage such that it is no longer working. It is not clear that the thieves accessed or tried to access either set of files.
No clear access attempted

Scenario #2: website/network breaches of security

As the result of implementing a new series of software applications at a small e-commerce company, the CTO discovers that one employee has access to all (5000) of their customers' credit card information through his desktop computer, where the employee has no "need to know" this information for his job function. When confronted, the employee professes to not knowing that he had such access, never mind having actually ever accessed this information.

The recently completed implementation means that it is not possible to assess whether access was ever made using the computer. Even if such access could be determined, the company is designed with an open-concept floor plan, such that anyone could have accessed the customer information.

Does this pass the material breach threshold to report?

Is there a real risk of significant harm and thus a need to notify?

Case Summary #2 - Additional Facts

The same e-commerce company, several months later, realizes that, due to human error, for the past two months the unsecured beta version of their new e-commerce website has been operating in production, such that the company has therefore been collecting customer credit card information through an unsecured site. While there is no evidence of any breach in the security of the database in either of the two months, there is evidence that at one point in the second month the network was accessed by an unauthorized person.

Case Study #2 – Additional Facts

As a result of investigating the breach of network security, it is determined that the cause of the breach was an ex-employee of the company.

How systemic is this breach?

Scenario #3: National Breach

A national luxury retail company, with stores across the country, suffers a loss of customer information at one office in Ontario. The information in question is the customer's contact information, and the fact that they are "VIP" customers. While this status is conferred on customers which spend more than a certain amount annually at the stores of the company, that specific monetary threshold is internally policy-driven and was not set out in the lost customer information.

Scenario #3 – Additional Facts

An individual informally determines that this breach has happened, and complains to the federal Privacy Commissioner. The Commissioner wants to determine if the company should have reported the breach to her office pursuant to Section 10.1(1), as being a "material breach of security safeguards". Only a few of the individuals in the customer information were identified as VIP's. However, based on the facts of the loss the federal Commissioner suspects that other offices in other provinces may have suffered a similar breach. To her knowledge, there has not yet been a relevant complaint made against the company in any of the other provinces. She would like to raise the issue with the other Commissioners, in order to assess the scope of the potential breach.

Can the OPC look at related breaches in other jurisdictions? Can the OPC ask other jurisdictions to assess?

Case Scenario #3 – Additional Facts

The company has determined that, based on the facts of the disclosure, it is not necessary to notify the VIP individuals of the privacy breach, on the basis that it is not reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

In the context, the federal Commissioner is not convinced that the company has made the correct decision.

Can the OPC use power to make public information management practices and notify individuals?

Appendix 4 - PIAC Legal Memo on Data Breach Class Actions in Canada

MEMORANDUM

To: John Lawford, Counsel, PIAC

Re: Summary of Canadian Class Action Data Breach Cases

QUESTIONS:

1) *Have data breach class action applications been filed in Canada?*

2) *How have courts addressed the issue of damages in these cases?*

CONCLUSIONS:

1) *Several class action applications against major corporations for data breaches have been filed in Canada in the recent past. Among those that have gained much public attention are: TJX Co (2008); Speevak v. CIBC (2010); and Larose c. Banque Nationale du Canada (2010). Recent data breach incidences occurring within the past 12 months (2011), include a case against Honda Canada, and the widely publicized Sony Playstation Case. An application against Honda Canada has been filed to the Ontario Superior Court of Justice by Flaherty Dow Elliot and McCarthy. An application against Sony Play Station has been issued by McPhadden Samac Tuovi LLP, but not yet filed.*

2) *TJX Cos and Speevak v. CIBC have both been resolved through settlement agreements between the companies and the consumers. Although in these cases breach-related expenses were considered in the determination of the benefits awarded, the issue of damages has not been directly addressed by the courts and remains a barrier to a successful data breach class action law suit. This was confirmed in Larose c. Banque Nationale du Canada, where the Court noted that under Quebec law, the fear of identity theft or fraud does not constitute harm or injury in and of itself and cannot provide a basis for a class action suit. In that case however, the application was authorized because there was evidence of harm which included evidence of actual identity theft as well as the fact that the National Bank did not offer credit monitoring services to affected clients.*

Data Breach Class Action Applications Filed in Canada

Research revealed three applications that have been filed in the recent past (*Churchman v. TJX Companies (2008); Speevak v. CIBC (2010);* and *Larose c. Banque Nationale du Canada)* and two that have been filed within the past year (*Scholes v. Honda Motor Company Ltd.* and *Maksimovic v. Sony PlayStation*). This section will provide a brief summary of these applications.

- ***Churchman v. TJX Companies (2008)***

On January 17th 2007, the TJX Companies (TJX), parent company of Winners and HomeSense, announced that the computer systems responsible for processing and storing consumer transaction information, had been subject to a security breach, compromising the sensitive data contained within. The breach occurred between July 2005 and January 2007 and affected approximately 45.6 million credit and debit card accounts.[270] Following the announcement by TJX, six class action suits were brought against the company on behalf of Canadians, claiming that TJX failed to maintain adequate security for consumer information and failed to inform affected consumers in a timely manner.[271] Without admitting guilt or wrongdoing, TJX entered into a proposed settlement agreement with plaintiffs in the United States. This agreement was later approved by Canadian Courts at a fairness hearing.[272]

The approved settlement agreement included the following benefits for qualifying members in Canada:[273]

> (a) for those class members whose driver's license or government identification number was determined to have been compromised (about 330 class members with addresses in Canada):
>
> (i) Credit monitoring and identity theft insurance,
>
> (ii) Reimbursement for the replacement cost of drivers' licenses that were replaced during a defined time as a result of the intrusion.
>
> (b) for class members who shopped at TJX stores (including Winners and HomeSense in Canada) during defined time periods and who incurred out-of-pocket costs and/or lost time as a result of the intrusion, up to two vouchers for $30 each, depending on documentation;
>
> (c) TJX/Winners/HomeSense will hold a one time special event where all store items will be reduced by 15%; and

[270] Wendy Gross, "TJX Enters Into Proposed Settlement Agreement of Customer Class Actions", online: McCarthy Tetrault <http://www.mccarthy.ca/article_detail.aspx?id=4103>
[271] *Ibid.* See also: *Churchman and Jin v. The TXJ Companies Inc.* (Statement of Claim filed in the province of Manitoba at The Queen's Bench Winnipeg Centre on July 31st 2007)
[272] *Ibid.* See also: *Wong v. TJX Companies* [2008] O.J. No. 398. [*Wong v.TJX*]
[273] *Ibid. Wong v.TJX* at para 6.

(d) TJX shall have an ombudsman available for a defined time period at a toll free number to assist customers with any questions in respect of card cancellations, credit theft, etc.

This agreement was criticized as many believed that by offering marketing gimmicks and small sales vouchers, TXJ did not suffer significant financial repercussions. Concern was also expressed regarding the speed at which the agreement was reached, as many important issues pertaining to responsibility and liability for security breaches remained unresolved. [274]

- ***Speevak v. Canadian Imperial Bank of Commerce (2010)***

Between 2001 and 2004 various CIBC branches accidentally sent numerous faxes, containing personal information about CIBC's customers, to two companies, one located in Quebec and one in the United States. In 2005, the Privacy Commissioner found that CIBC failed to safeguard its clients' personal information from disclosure as required by the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*").[275] The Statement of claim alleged that the CIBC had breached its duty of confidentiality, was negligent to have done so, and that this in turn led to a breach of customers' privacy rights. [276]

Much like in the TSX case, the plaintiffs and the CIBC entered into a settlement agreement in 2009. Terms to the agreement included the following:[277]

- Following the receipt of a standardized claim form, the CIBC was required to make an offer of settlement to the class member. If the class member did not agree with the settlement proposed, they had the right to have their claim assessed by an independent arbitrator, paid for by the CIBC.
- The right to claim for identity theft any time in the future was preserved.
- Recoverable damages did not include punitive or aggravated damages.
- The CIBC was responsible for paying fees and disbursements of class counsel up to the date of mediation.
- 10% of any payment made to each class member was to be paid by the CIBC to the Class Proceedings Fund.
- The CIBC was required to pay $100 000 to a registered charity. In this case the charity selected was The Public Interest and Advocacy Centre (PIAC).

- ***Bordoff v. CIBC Asset Management Inc. (2010)***

[274] *Supra note 1.*
[275] *Speevak v. Canadian Imperial Bank of Commerce* [2010] O.J. No 770 [*Speevak v. CIBC*] at para 4-6. See also: *Speevak v.Canadian Imperial Bank of Commerce* (Statement of Claim filed in the province of Ontario to the Superior Court of Justice on February 4th 2005) and *CIBC's privacy practices failed in cases of misdirected faxes*, Incident Summary #2 2005, online: Office of the Privacy Commissioner of Canada < http://www.priv.gc.ca/incidents/2005/050418_01_e.cfm>
[276] *Ibid.* at para 8.
[277] *Ibid.* at para 27-37.

Between December 2006 and January 2007, the Canadian Imperial Bank of Commerce (CIBC) reported to that a package supposedly containing a portable computer disk drive holding personal information of more than 400,000 current and former clients of Talvest Mutual Funds a family of CIBC Mutual Funds, (Talvest) had been lost while being shipped from Quebec to Ontario.[278] The data in question had not been encrypted. Following this incident a class action proceeding was introduced in the province of Quebec by consumers affected by the breach.

Similarly to the previous cases, the Talvest case was resolved by the means of a settlement agreement between the parties.[279] The agreement arrived at in 2010, provided for the following compensation:

- For all individuals whose personal information was identified by Talvest as having been saved or contained on a disc drive which went missing on or about December 13th, 2006 and who had sustained documented monetary loss arising directly from the unauthorized use of this personal information (non-monetary damages such as inconvenience and stress were excluded), could have their claims assessed by Talvest for compensation. If the class member did not agree with the settlement proposed, they had the right to have their claim assessed by an independent arbitrator, paid for by Talvest.
- Talvest also agreed to donate 180 000$ to three charitable institutions, the Walrus Foundation, The Canadian Museum for Human Rights and the Segal Cancer Centre of the Jewish General Hospital in Montreal.

- ***Larose c. Banque Nationale du Canada (2010)***

Due to the theft of three laptop computers from its head offices in Montreal, the National Bank of Canada (National Bank) lost personal mortgage information belonging to some 225 000 clients.[280] In the days following the incident, the National Bank attempted to protect clients privacy rights by initiating several steps including; issuing a press release, sending a letter to clients through the post, filing a notice with credit bureaus, and issuing a note in the clients bank profile.[281] In addition to these steps the National Bank informed the Federal Privacy Commissioner of the breach and committed to compensating any client who, as a direct result of the breach, became a victim or fraud or identity theft.[282] Despite these efforts however, a

[278] *Commissioner initiates safeguards complaint against CIBC*, PIPEDA Case Summary #2008-395, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/cf-dc/2008/395_20080925_e.cfm > See also: *Gloria Bordoff* v. CIBC *Asset Management Inc*, (Statement of Claim filed in the province of Quebec to the Superior Court in the District of Montreal, on January 3, 2007) online: cba.org < http://www.cba.org/classactions/class_2007/quebec/pdf/2007-01-23_CIBC.pdf>

[279] *Gloria Bordoff v. CIBC Asset Management INC.* [2010] Q.J. No. 10334 and *Settlement Notice Talvest Mutual Funds re: Talvest Backup Computer Security Disc Settlement* online: merchantlaw.com < http://www.merchantlaw.com/classactions/talvest_bordoff.php>

[280] *Larose c. Banque Nationale du Canada* [2010] J.Q. no 11510 para 2. [*Larose c. BNC*]

[281] *Ibid* at para 5.

[282] *Ibid.* at para 6.

class action suit was filed against the bank for negligence in the retention and protection of clients' personal information, failing to offer credit monitoring service to affected clients, undue delay in informing clients of the breach, inadequate choice of communication methods to inform clients of the breach and failure to identify account co-holders of the breach.[283]

Although this case has not yet been heard before a court, nor has a settlement agreement between parties been reached, in the preliminary authorization granted by the Quebec Superior Court, it was noted that under Quebec law, the fear of identity theft does not in and of itself constitute harm or injury, evidence of actual theft must exist. The case was approved as there was evidence that one of the plaintiffs had in fact become a victim of identity theft.[284] Other evidence of injury cited in the decision included the Bank's failure to offer credit monitoring and related services to class members.[285]

- ***Scholes v. Honda Motor Company Ltd.***

Around March 13th, 2011, Honda Canada (Honda) discovered that clients' personal information had been misappropriated. Only on May 13th, however, did Honda advise the plaintiffs that a data breach had occurred.[286] Among the allegations advanced by the plaintiffs was that Honda failed to; have adequate and necessary data security on place at the time of the breach, notify its customers regarding the breach in a reasonable amount of time. According to the statement of claim these omissions exposed class members to various harms including identity theft and harassment.

This application has recently been filed and as such neither a settlement, nor a decision has been reached at this time.

- ***Maksimovic v. Sony PlayStation***

In April of 2011, Sony announced that personal information of 77 million PlayStation and Qriocity accounts worldwide, 1 million of which are in Canada, had been compromised. Sony was allegedly aware that such information had been stolen but failed to advise users in a timely fashion.[287] According to a press release issued by McPhadden Samac Tuovi LLP, the only compensation offered by Sony to Canadian users, was a 30 or 60 day free memberships on its

[283] *Ibid.* at para 7.
[284] Patrick Flaherty, Wendy Matheson *et al.,* "Privacy Class Actions Are Here, But Do We Need Them?", *Canadian Privacy Law Review*, 8:2 (January 2011) at 17 online: Torys.com < http://www.torys.com/Publications/Documents/Publication%20PDFs/AR2011-2.pdf> See also: *Larose c. BNC* at para 27.
[285] *Supra* note 9 at para 24.
[286] *Scholes v. Honda Motor Company Limited* (Statement of claim filed in the province of Ontario to the Superior Court of Justice on May 27th 2011) para 14-18.
[287] McPhadden Samac Tuovi LLP, News Release/Communiqué, "Canadian Sony PlayStation Network Class Action" (2 May 2011) online: <http://www.mcst.ca/ClassActions/ClassActionsHome/SonyPSN/>. See also: McPhadden Samac Tuovi LLP, News Release/Communiqué, "Sony PlayStation Proposed Class Action Update" online: < http://www.mcst.ca/ClassActions/ClassActionsHome/SonyPSN/>

PlayStation network. The same press release states that Sony had advised American users about the availability of free credit reports, but had not yet provided Canadian users with similar information. At this time, the Statement of Claim has not yet been filed.

How courts have addressed the issue of damages in data breach class action lawsuits

A general trend that emerges from the cases summarized above appears to indicate that generally most class action suits related to a data breach are resolved by the means of a settlement agreement. Although breach-related expenses have been considered in the determination of the benefits awarded in such agreements, the issue of damages, and what constitutes damage in data breach cases, has not been directly addressed by the courts and remains a barrier to a successful data breach class action suit. *Larose c. Banque Nationale du Canada* offers some insight as the Court states that the fear of identity theft or fraud does not constitute harm or injury in and of itself and cannot provide a basis for class actions. Again, in that case the Court authorized the suit because there was actual evidence of harm, which included the fact that the National Bank did not offer credit monitoring services as well as evidence of actual identity theft. It remains to be seen if this determination will be applied in a court of law.