Information Security Breaches & The Law

Type here and press enter t

- Home
- About »
- "Security Breaches" Library

Canada May Soon Have a Data Breach Law

Posted by "Security Breaches" Administrator on 05/06/2010 · Leave a Comment

Canadian Industry Minister Tony Clement introduced a bill on May 25, the *Safeguarding Canadian's Personal Information Act* (C-29), which would amend Canada's national privacy legislation, the *Personal Information and Electronic Documents Act of 1998* ("PIPEDA"). C-29 would introduce a security breach disclosure (also called "notification" in the United States) requirement in PIPEDA. Canada does not yet have such a law, contrary to the United States where the majority of states have enacted data breach notification statutes.

PIDEDA protects Canadians' personal information and applies to every organization in the private sector collecting personal information on Canadians in the course of business. PIPEDA became law more than ten years ago, in April 2000. It includes a provision for a mandatory review by Parliament every five years. A report on PIDEDA by the Canadian House of Commons Standing Committee on Access to Information, Privacy, and Ethics was published in 2007.

The Committee noted that, while breach notifications were only voluntary in Canada, many U.S. states have passed breach notification legislation. The Privacy Commissioner herself recommended an amendment to PIPEDA to create a breach notification provision. C-29 has just now been introduced three years after the Committee's recommendation. The Committee had issued the following three recommendations regarding breach notification provisions:

Recommendation 23:

The Committee recommends 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.

Recommendation 24:

"The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner."

Recommendation 25:

The Committee recommends 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.

C-29 maintains the distinction between notifications to the Privacy Commissioner and notifications to the individuals affected by the breach. However, C-29 would not give the Privacy Commissioner the power to determine whether the breach has affected individuals. This judgment is left to the organizations.

Reporting security breaches to the Privacy Commissioner of Canada (New section 10.1 of Law C-29)

An organization will have to report a "material breach of security safeguards involving personal information under its control" to the Privacy Commissioner of Canada. The amendment does not contain any penalties for organizations that fail to report these breaches, nor does the amendment contain any incentives for organizations to do so. However, with the publicity surrounding the bill, organizations would have at least a good reason to protect personal information to avoid potentially embarrassing revelations in the media that their data security program is less than adequate.

Also, companies are left free to determine whether the breach is indeed "material." In order to assess if it is material, the organization must consider three factors: 1) the sensitivity of the personal information, 2) the number of individuals whose personal information was involved, and 3) whether the organization assesses that the cause of the breach, or the pattern of breaches, indicates a systemic problem.

It seems that these factors are cumulative, and thus all three factors must be considered before the organization has to report a security breach to the Privacy Commissioner. This does not put much pressure on organizations, which may decide, whether in good faith or in bad faith not to report a particular security breach to the Privacy Commissioner.

The Privacy Commissioner of Canada had investigated the TJX company in September 2007, after a breach of TJX's computer networks exposed the credit card data and personal information of 45

million individuals, amongst them many Canadians. After auditing TJX, the Office of the Privacy Commissioner recommended the company to monitor its systems more closely, and to use higher encryption standards, which TJX did. However, no fines were imposed at that time.

In contrast, several U.S. states authorize the state attorney general to remedy a violation of a data breach notification requirement (New York, Florida, and Pennsylvania among them). Some states authorize a private right of action (Louisiana and Nevada). The U.S. statutes do not have a similar reporting provision, as the U.S. does not have a Privacy Commissioner or its equivalent. Since there is no preemptive federal security breach notification law, it is the state law of the place where the breach physically occurred which will be applicable, but other state laws will be applicable as well, if the breach exposed the personal information of their own citizens. Therefore, a company collecting personal information all over the United States must be familiar with every state security breach law.

Reporting security breaches to the affected individuals (New section 10.2 of Law C-29)

Organizations also will have to notify individuals "as soon as feasible," if it is reasonable to believe that this breach of security "creates a real risk of significant harm to the individual." The bill defines "significant harm" as "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."

The factor an organization must use to assess whether there is a real risk of significant harm to the individual is "the sensitivity of the personal information involved in the breach." PIPEDA does not, however, define what is sensitive information. Its section 4.3.4 considers that some information, such as medical information, is always sensitive, but also considers that "any information can be sensitive, depending on the context" and "the probability that the personal information has been, is being or will be misused."

Compared to the U.S .statutes, C-29 is much more lenient. Most U.S. state laws require organizations to send a notice to an individual even if there is only a possibility that the security of their data may have been compromised. The slightest doubt triggers sending a notice, whereas, if C-29 were enacted, even if an organization is certain that there has been a security breach, it may still decide not to send out a notice because it would assess that there is no real risk of significant harm.

However, C-29 has a very interesting definition of what may constitute harm, which could influence other legislators. It was drafted this year, just after the numerous Facebook privacy policy changes, whereas the U.S. statutes were mainly enacted to protect the individuals against identity theft. Social networking sites are now considered the big privacy threat in the public's eye, as identity theft used to be a few years ago, even though identity theft remains a prevalent crime. C-29 indeed lists identity theft as one of the "significant harms" which may be created by a breach of security, but it also lists "humiliation" and "damage to reputation." Our reputation online is composed of the myriad of personal data available about us, aggregated by websites such as search engines and profile building companies (think Google and ZoomInfo). Daniel Solove wrote in his book about the future of reputation that "our reputations are forged when people make judgments based upon the mosaic of information available about us." So a reputation may be shattered either by true, but negative information about the individual, or by negative and untrue information about that person. Both types

of information, if leaked by social networking sites, could damage a reputation.

If C-29 is enacted and effectively amends PIPEDA, it will be interesting to see if there will soon be lawsuits against social networking sites that, because of a security breach, expose humiliating personal data (see an example here), and how the Canadian courts will interpret "humiliation."

What impact could the PIPEDA amendment have on foreign companies with affiliates in Canada?

Foreign companies with affiliates in Canada should follow these developments closely, and anticipate that C-29 will be enacted.

As the public becomes more aware of their personal consequences of security breaches, they will demand answers from companies should breaches occur. To avoid damaging public relations problems, companies will have an incentive to plan steps to mitigate potential breaches and be forthcoming in their responses to the public.

First and foremost, companies should candidly assess whether they are at risk, by checking the internal procedures used to gather and secure customer information, and the security of their information systems.

Companies should set their own formal, written, internal benchmarks to be used to decide whether a breach should be reported to the Privacy Commissioner (sensitivity of the information, the number of people affected, and whether or not the breach indicates a systemic problem), and to the public (real risk of significant harm to the individual).

Employees should also be informed of this new security breach notification requirement, and be trained appropriately, so they can detect them quickly, and know how to report them.

C-29 does not contain penalties for not notifying authorities or the public. So, the incentive for disclosing security breaches is related primarily to the potential for bad publicity, and loss of good will. Indeed, failing to disclose a security breach, if that breach is later revealed in the media, could lead to a significant loss of public confidence in the organization and its brands. Because of the publicity given to the new bill in the media, the general public will become more aware of the threat that a security breach can be harmful to them. Therefore, companies should be mindful of communicating effectively to the public on this subject. Organizations could use C-29 as a basis to plan responses and communicate to their customers and the public that they are mindful of protecting their personal data.

C-29 is Canada's first attempt at adding a security breach requirement to the nation's privacy laws. However, the bill does not contain penalties and damages for organizations failing to disclose security breaches. Will this "honor-system" type of law be efficient in forcing organizations to develop or review their information security programs?

Marie-Andrée Weiss & Cédric Laurant

Links:

Bill C-29, An Act to amend the Personal Information Protection and Electronic Documents Act (May 25 2010)

David Fraser, "Markup of Bill C-28 and Bill C-29 Amendments to PIPEDA," Canadian Privacy Law Blog, May 26, 2010 (a very informative markup version of PIPEDA, complete with the new amendments).

List of United States state security breach notifications laws (updated until April 12, 2010)

Federal Trade Commission, Consumer Sentinel Databook (for Jan.-Dec. 2009), Feb. 2010

Possibly related posts: (automatically generated)

- National Briefing
- How Canada really avoided a housing bubble
- The ongoing war against cybercrime – CNN.com

Filed under Comments, ENGLISH · Tagged with Canada, security breach disclosure, security breach notification, data breach notification statute, PIPEDA, Privacy Commissioner of Canada, C-29, material breach, TJX, United States, preemption, significant harm, sensitive information, Facebook, social networking sites, identity theft, reputation, damage to reputation, online reputation, profile building companies, search engines, security breach, humiliation, potential breaches, information system, customer information, systemic problem, bad publicity, public confidence

The Safe Harbor Framework: not a "safe harbor" anymore for US companies? German expert body insists on stronger compliance stance

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <pre> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

- [ ] Notify me of follow-up comments via email.

- [ ] Notify me of site updates

- **Recent Posts**

  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive
  - Are 'clouds' located outside the European Union unlawful?
  - The Safe Harbor Framework: not a "safe harbor" anymore for US companies? German expert body insists on stronger compliance stance
  - Canada May Soon Have a Data Breach Law

- **Recent News on Security Breaches**

  - "Consumer View: Staying Safe from Cyber Snoops" (FCC, June 11, 2010) Recent news reports have focused attention on a growing concern: The ways in which wireless and WiFi networks can make consumers' private data accessible. (…)
  - "Sécurité des données personnelles : les entreprises ne font pas face" (ITR News, 9 juin 2010) L'étude souligne le fait que, en dépit de ce que croient beaucoup d'entreprises, le fait de respecter la réglementation en vigueur ne suffit pas à assurer une protection efficace des données. En effet, alors que 70 % des sondés affirment (…)
  - "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program" (FTC, June 24, 2010) The FTC's complaint against Twitter charges that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had (…)
  - "UK headed for data breach disclosure law within four years" (siliconcom, July 16, 2010) "According to lawyers at law firm Field Fisher Waterhouse, legislation requiring organisations to notify the relevant authorities as well as individuals affected in the event of a serious security breach will be introduced across Europe."
  - "Survey: 87 per cent of UK businesses favour mandatory disclosure of data breaches"

(Secure Business Intelligence, July 6, 2010) 87 per cent of organisations believe that data breaches should be revealed when sensitive data about the public is exposed. Revealed, but to whom?

- "Putting a Private Detective in Your Laptop" (New York Times, June 16, 2010) "According to a study by the Ponemon Institute, 12,000 laptops are lost each week in American airports (…) You can keep an eye on your devices and not leave them visible and unattended, but they might best be protected with some software."
- "Credit Card Hackers Visit Hotels All Too Often" (New York Times, July 5, 2010) Hotels are a favorite target of hackers. A study released this year by data-security consulting company SpiderLabs found that "38 % of the credit card hacking cases last year involved the hotel industry".
- Ponemon Institute: First Annual Cost of Cyber Crime Study (ArcSight, July 26, 2010) "The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount (…
- Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (FTC, July 27, 2010) "The FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash that contained consumers' personal information such as pharmacy labels and job applications. (…)"

- **Tag Cloud**

adequate level of data protection Article 29 Data Protection Working Party Binding corporate rules Bundesdatenschutzgesetz C-29 Canada cloud computing confidentiality contractual clauses damage to reputation data breach notification statute data security Düsseldorfer Kreis encryption EU Directive 95/46/EC European Commission European data protection authorities European Union external audit Facebook German Federal Data Protection Act Germany identity theft integrity material breach online reputation personal data PIPEDA preemption Privacy Commissioner of Canada profile building companies reputation Safe Harbor Framework Safe Harbor self-certification search engines security breach security breach disclosure security breach notification self-regulation sensitive information sensitive personal information significant harm social networking sites TJX United States

- **Blog Authors**

- **Disclaimer & Comments Policy**
  - Disclaimer & Comments Policy
- **Authors' upcoming talks & conferences on information security & legal issues**
  - Cédric Laurant: "Seminario internacional: seguridad de la informacion, cibercriminalidad y propiedad intelectual" (international seminar on information security, cybercriminality and intellectual property) IUSTIC & Universidad Pontificia Bolivariana (Medellin, Colombia – Aug. 3-12, 2010)
  - Cédric Laurant: II Congresso Crimes Eletrônicos e formas de proteção (2nd Congress on Cybercrimes and Protection Measures) Federação do Comércio do Estado de São Paulo (Sao Paulo Chamber of Commerce), Sao Paulo, Brazil – Sept. 27-28, 2010
  - Cédric Laurant: "Legal Developments and Relevant Court Decisions in Latin America" High Technology Crime Investigation Association (HTCIA) International Conference (Atlanta, GA-USA – Sept. 20-22, 2010)
- **Tweets (last 10)**
  - List of recent surveys and reports on security breaches: http://bit.ly/9VamhE - tweeted 22 hours ago
  - ArcSight & Ponemon Institute: release of "1st Annual Cost of Cyber Crime Study" http://bit.ly/d1Us8e - tweeted 22 hours ago
  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive. New blog posting at http://bit.ly/aOG3cY #in - tweeted 1 week ago
  - "Are ‘clouds’ located outside the European Union unlawful?" New blog posting. http://bit.ly/djUNCy #in - tweeted 1 week ago
  - "The Safe Harbor Framework: not a 'safe harbor' anymore for US Companies?" New blog

posting. http://lnkd.in/ShwMWj - tweeted 2 weeks ago
- "The Safe Harbor Framework: not a "Safe Harbor" anymore for US Companies?" New blog posting: http://wp.me/pW5Fc-1D - tweeted 2 weeks ago
- FTC's proposed consent agreement with #Twitter: company misrepresented its security measures. http://bit.ly/cF8LNk - tweeted 1 month ago
- Your "private" tweets are... public! #Twitter prone to security breaches, FTC says in consent agrmt. Com'ts requested. http://bit.ly/axKpnV - tweeted 1 month ago
- FTC's 1st case agst social netwkg website: #Twitter failed to safeguard users' PII despite promises in privacy policy http://bit.ly/ajUG9J - tweeted 1 month ago
- Backing up data is one thing, encrypting the backups another, but restoring the encrypted data, even more complex. http://bit.ly/bGgQt2 - tweeted 1 month ago

- **Subscribe to this blog by e-mail**

  Enter your e-mail address here to subscribe to this blog and receive notifications of new posts by e-mail.

  Sign me up!

-

- **Counters**

- 

Information Security Breaches & The Law ·

Blog at WordPress.com. Theme: Structure by Organic Themes.