Assignment 2; isec3050-701; nscc

Richard Rennehan; October 28, 2018

BREACH NOTIFICATION STANDARDS FOR SECTORS WITHIN CANADA AND USA

Contents

[Introduction 2](#_Toc528532513)

[Canadian Privacy Breach Standards 3](file:///E:\NSCC\Data%20Analytics%20Year%202\Ethics%20and%20Law\Rennehan-Richard-ISEC3050-701-As2.docx#_Toc528532514)

[Canadian Public Sector 4](#_Toc528532515)

[Canadian Private Sector 6](#_Toc528532516)

[British Columbia 6](#_Toc528532517)

[Alberta 8](#_Toc528532518)

[Canadian Health Care Sector 9](#_Toc528532519)

[Ontario 9](#_Toc528532520)

[Newfoundland 10](#_Toc528532521)

[USA Privacy Breach Standards 11](file:///E:\NSCC\Data%20Analytics%20Year%202\Ethics%20and%20Law\Rennehan-Richard-ISEC3050-701-As2.docx#_Toc528532522)

[USA Public Sector 12](#_Toc528532523)

[USA Private Sector for 2 States 13](#_Toc528532524)

[California 13](#_Toc528532525)

[Georgia 16](#_Toc528532526)

[USA Health Care Sector 17](#_Toc528532527)

[Federal HIPAA 17](#_Toc528532528)

[California Health Privacy Law 19](#_Toc528532529)

[Review of Privacy Breach Laws 20](file:///E:\NSCC\Data%20Analytics%20Year%202\Ethics%20and%20Law\Rennehan-Richard-ISEC3050-701-As2.docx#_Toc528532530)

[Comparisons 21](#_Toc528532531)

[New Canada Mandatory Breach Notification Law 23](#_Toc528532532)

[Conclusions and Outlook 25](#_Toc528532533)

[References 26](#_Toc528532534)

# Introduction

Data and privacy breaches are now commonplace in today’s digital information age. In fact, there is a hacker attack every 39 seconds in the United States. To put it into a broader perspective, one in three Americans are affected by a data privacy breach every year. The chairman, president and CEO of IBM, Ginni Rometty, has said: “Cyber crime is the greatest threat to every company in the world.” (Devon Milkovich, 2018)

This raises the question of where current data breach laws stand across Canada and the United States. Are there any unifying standards of practice in the event of a data breach, and will the standards have to be raised? This document will compare current privacy breach laws for a handful of federal, private, and health care sectors within Canada and the United States as of October 28, 2018.

# Canadian Privacy Breach Standards

## Canadian Public Sector

To summarize breach laws for government institutions in Canada, both affected individuals and privacy regulators are to be notified of a breach of sensitive information as soon as feasible (Government of Canada, 2014)

As of October 28, 2018, Canada has no federal legislation for the timing and content of breach notifications. Instead, each province has their own specific legislation for data privacy in the public sector. However, guidelines for privacy breaches for government institutions can be found online at the Government of Canada site (2014)

The guidelines recommend that with any breach of personal or private information, affected individuals should be notified as soon as feasible (Government of Canada, 2014). A breach of personal information falls under personal information that has been wrongfully disclosed, stolen or lost. Personal information is defined as financial or medical information, or personal identifiers like Social Insurance Numbers (Government of Canada, 2014). Here’s a list of what the guidelines say to include in a privacy breach notification letter:

* General description of incident, including date and time
* Source of breach (institution, contracted party, or a party to a sharing agreement)
* A list of personal information that has or may have been compromised
* Description of measures taken or to be taken to retrieve personal information, contain the breach, and prevent reoccurrence.
* Advice to the individual to mitigate risks of identity theft or to deal with compromised personal information (e.g., Social Insurance Number).
* The name and contact information of an official at the institution with whom individuals can discuss the matter further or obtain assistance.
* A reference to the effect that the OPC has been notified of the nature of the breach and that the individual has a right of complaint to that office, when applicable.
* Inform affected individuals of developments as the matter is further investigated and outstanding issues are resolved.

(Government of Canada, 2014)

It may also be necessary to report to the Office of the Privacy Commissioner and the Treasury Board of Canada Secretariat. The site says the following about reporting to these regulators:

It is necessary to report any breach involving material information to the Office of the Privacy Commissioner (OPC) and the Treasury Board of Canada Secretariat (TBS). A material breach is a considered a breach which involves sensitive permission information and could reasonably be expected to cause serious injury or harm to individuals affected. The second of the two prerequisites may be bypassed if the breach has affected a large number of individuals. Sensitive personal information as defined here includes but is not limited to: medical information, criminal history, financial information, race/ethnic origin, and religious or political beliefs. Serious injury or harm to the individual as defined includes identity theft, fraud, material loss, or lasting harm or embarrassment on the individual affecting their career, reputation, safety, health, and financial position.

(Government of Canada, 2014)

## Canadian Private Sector

Business performing in the private sector in Canada are subjected to either the federal Personal Information Protection and Electronics Documents Act (PIPEDA) or to any privacy laws exclusive to the province. It’s important to note that PIPEDA currently does not have any legislature requiring breach notification. The provinces that have their own privacy legislation are British Columbia, Alberta, and Quebec, and are often stricter than PIPEDA. This section will cover privacy laws set for British Columbia and Alberta, as they appear to be the only two mentioning breach notification.

### British Columbia

According to the *Privacy Breaches: Tools and Resources* guide (2012), “Notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them” and that notification should occur as soon as possible following the breach.

The guide (2012) describes a privacy breach as when there is unauthorized access, collection, use, disclosure or disposal of personal information.” After containing the breach, the guide (2012) recommends evaluating the risks based on:

* Personal information involved
* Cause and extent of the breach.
* Individuals affected by breach
* Foreseeable harm from breach

The guideline (2012) recommends reviewing the risk assessment to determine to notify individuals. Any form of direct notification is accepted, including phone, letter, and in person. The following information should be included in the notification, according to the guideline document (2012):

* Date of breach
* Description of breach
* Description of information inappropriately accessed, collected, used, or disclosed
* Risk(s) to individual caused by breach
* Steps taken so far to control or reduce harm
* Future steps planned to prevent further privacy breaches
* Steps the individual can take to further mitigate risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's license number
* Contact information of an individual within the organization who can answer questions or provide further information
* Privacy Commissioner contact information and fact that individuals have a right to complain to the office of the Information and Privacy Commissioner. If organization has already contacted privacy commissioner, include this detail in the notification letter.

Aside from notifying individuals, the guidelines specify who may have to be contacted following a privacy breach. Here’s what the guideline (2012) specifies:

* Police: If theft or other crime is suspected
* Insurers or others: If required by contractual obligations
* Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies
* Other internal or external parties not already notified: Your investigation and risk analysis may have identified other parties impacted by the breach such as third-party contractors, internal business units, or unions.

### Alberta

Alberta is noteworthy for being the only province with mandatory breach notification laws following a breach of personal information to this day.

According to the Office of the Information and Privacy Commissioner of Alberta site (n.d.), it is mandatory for an organization to notify the Commissioner without reasonable delay of any privacy breach that may result in a real risk of significant harm to the individual. A breach notification form is provided where details are filled in about the breach, organization, whether individuals have been notified, information involved, harm, risk assessment, and risk mitigation.

A similar webpage on the Office of the Information and Privacy Commissioner of Alberta site clarifies that the Commissioner determines whether notification to individuals is required based on a real risk of significant harm. If so, the commissioner publishes the decision for the company to follow.

## Canadian Health Care Sector

According to the Officer of the Privacy Commissioner in Canada’s (2018) article on summary of privacy laws in Canada, only 4 provinces in Canada have health-related privacy acts. These are Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia. They are stated to be similar in content to PIPEDA.

This section will display health-related privacy laws for Ontario and Newfoundland.

### Ontario

Ontario is covered under the *Personal Health Information Protection Act* (2004).

Under the Personal Health Information Protection Act, custodians must notify the information and privacy commissioner of Ontario about breach of private health information. Any individuals affected must be notified at the first reasonable opportunity of the breach.

The only content requirement in the breach notification statement to the individual is a notice stating the individual is entitled to make a complaint to the Commissioner under Part VI. 2016, c. 6, Sched. 1, s. 1 (4).

### Newfoundland

Newfoundland is covered under the *Personal Health Information Act* (2018).

According to the Personal Health Information Act of Newfoundland (2018), a custodian shall notify the commissioner following a material breach. A material breach is defined as the unauthorize collection, use, or disclosure of personal health information. From there, the commissioner may recommend notification to any individuals affected at the first reasonable opportunity.

Notification to the individual may be determined not necessary if the breach will not have an adverse impact upon:

* The provision of health care or other benefits to the individual
* The mental, physical, economic, or social well-being of the individual

# USA Privacy Breach Standards

## USA Public Sector

Surprisingly, there are currently no federal legislatures specifying timing, audience, and contents of breach notifications in the US, even for all federal institutions. Legislation on privacy breaches is left to state law, with the exception of South Dakota and Alabama. South Dakota and Alabama are the only states that do not require breach notification (Geoffrey Elkins, n.d.).

Many advocates agree that there should be a national data breach standard in the US. Reflecting on the Equifax breach of 2017, Mr. Rotenberg said: “I think our recent experience with Equifax demonstrates the need for prompt breach notification.” (Gonzalez, 2018, para. 4). While some companies like Equifax may delay their notifications, there have been cases where companies outright attempted to hide breaches as well. In 2016, Uber attempted to hide a breach by paying the hackers $100,000 to delete the information of the 57 million customers and drivers they stole (Gonzalez, 2018, para. 5). With a stricter, national standard, individuals can be aware of breaches sooner and take action to protect themselves in time before disaster strikes.

## USA Private Sector for 2 States

Unlike Canada, most areas of the United States require notification of privacy breaches. The required timing, audiences, and content of privacy breach notifications vary state to state. What constitutes as a privacy breach also varies. The biggest similarity, though, is that they all use similar phrasing for timing of the notification: “the most expeditious time possible and without unreasonable delay.” (Geoffrey Elkins, n.d., para. 3).

This section will compare the breach notification laws in the states of California and Georgia. California was chosen because it is home to numerous technology companies. Georgia was chosen because the Equifax headquarters are located in the state.

### California

To summarize California’s breach notification laws, any breach of personal information must be disclosed as soon as feasible to affected individuals and, if more than 500 California residents are affected, to the Attorney General as well (Baker & Hostetler, 2018).

The Baker & Hostetler site (2018) states the following about triggering breach notification: “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 entity.” Unlike many other states, where the breach of encrypted information does not require notification, encrypted information can also trigger notification, providing the encryption key or security credential to unencrypt it is also compromised. (Baker & Hostetler, 2018).

Regarding timing, the site states:

For persons/businesses that acquire, own or license data, disclosure

shall be made in the most expedient time and manner possible and

without unreasonable delay, consistent with the legitimate needs of law

enforcement or any measures necessary to determine the scope of the

breach and to restore the reasonable integrity of the data system.

The format for breach notifications in California may be the strictest of all. The law site for BakerHostetler law firm (2018) states the following:

Breach notification to California residents must be in written form, using plain language in no smaller than 10-point type. The notification shall be titled “Notice of Data Breach,” and use the following clearly and conspicuously display Breach notification to California

residents must be in written form, using plain language in no smaller than

10-point type. The notification shall be titled “Notice of Data Breach,” and

use the following clearly and conspicuously displayed headings:

(1) “What Happened”;

(2) “What Information Was Involved”;

(3) “What We Are Doing”;

(4) “What You Can Do”; and

(5) “For More Information.”

Breach notifications in California also require the following elements as stated from the BakerHostetler site (2018)

(1) the date of the notice;

(2) the name and contact information of the person reporting a breach;

(3) a list of the types of personal information likely impacted; and

(4) if the breach exposed a Social Security number or a driver’s license or

CA identification card number, the toll-free telephone numbers and

addresses of the major credit reporting agencies

Additional information may be provided as a supplement to the notice.

If the person or business providing the notification was the source of the

breach and the breach exposed or may have exposed a Social Security

number or a driver’s license or CA identification card number, an offer to

provide appropriate identity theft prevention and mitigation services, if

any, shall be provided at no cost to the affected person for not less than

12 months, along with all information necessary to take advantage of the

offer.

The notice must also include the following information if such information

is possible to determine before sending the notice:

(1) the date, estimated date, or date range of the breach;

(2) whether notification was delayed as a result of a law enforcement

investigation; and

(3) a general description of the breach incident.

### Georgia

According to Perkinscoie (2018), Georgia requires notification of affected individuals breach of unencrypted personal information without unreasonable delay, and if more than 10,000 residents of Georgia are affected, to all consumer reporting agencies as well.

The Perkinscoie (2018) site references the definition of a security breach as the following:

An unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality, or integrity of PI of such individual maintained by an Entity. (para. 2)

Like many other states, Georgia’s timing of notification is as follows:

The notice 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. (Perkinscoie, 2018, para. 6)

Interestingly, there appear to be no regulations or laws impacting how the notification letter must be formatted or what it must include.

## USA Health Care Sector

Health privacy laws in the United States fall into two categories: Federal and state. The federal privacy legislature is known as HIPAA (health insurance portability and accountability act).

There are a couple rules to whether federal legislature or state legislature on health privacy supersedes the other or not. According to David Humiston (2002), the following rules take place:

* Federal HIPAA law supersedes conflicting state law
* State law takes effect only if there is no HIPAA provision on a specific subject, if state law is stricter, or if there is an exception under HIPAA.

This section will look at federal HIPAA laws on privacy breach notification and California health privacy law to give an idea on what to expect.

### Federal HIPAA

According to *Centers for Medicare & Medicaid Services* (2016) on HIPAA breach notification rules:

HIPAA breach notification rule requires covered entities to notify affected individuals, the Department of Health & Human Services (HHS), and in some cases, the media of a breach of any unsecured personal health information. Notifications must be provided without unreasonable delay and no later than 60 days following discovery of a breach.

The hhs.gov site (2013) specifies the requirements for individual notice. The notification must be in written form, by first-class mail, or alternatively, by e-mail if the affected individual agreed to receive electronic notices (hhs.gov, 2013). Regarding content and timing, here’s what hhs.gov (2013) states:

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

Unique to HIPAA, breaches with over 500 residents affected are required to provide notice to prominent media outlets serving the state or jurisdiction (hhs.gov, 2013). The same rules on timing apply as with notification to individuals.

In addition, it is required to notify the Secretary of breaches of unsecured protected health information (hhs.gov, 2013). If the breach affects over 500 people, the notice to secretary must be provided without unreasonable delay and no later than 60 days following the breach (hhs.gov, 2013). If the breach affects less than 500, the entity may report all breaches with less than 500 affected on an annual basis. The reports are due no later than 60 days after the end of the calendar year in which the breaches are discovered (hhs.gov, 2013)

### California Health Privacy Law

Many of the regulations from HIPAA and California’s private sector apply to breach of personal health information in California. There are a few exceptions, though.

Section 1280.15 of the California Health and Safety Code requires notifying the individual no later than 15 business days of any unlawful or unauthorized access to, or use or disclosure of, their medical information. This is an example of a law that bypasses the HIPAA equivalent as it is stricter.

# Review of Privacy Breach Laws

# Comparisons

Timing stipulations for each sector covered are very similar among each sector. Many sectors shared similar ideas of requiring notification as soon as feasible and without unreasonable delay. However, the HIPAA was the only legislation which actually had a time limit, of which, was 60 days following the breach of more than 500 individuals. Nearly all of the legislations covered specifically mentioned allowing a delay if the notification will otherwise impede a criminal investigation.

Many sectors shared similar wording on the breach having a “real risk of significant harm” to the individual to warrant a breach notification.

The biggest difference between each sector, though, is what is required on the breach notification. Table 1 shows the differences between each sector based on content required in the breach notification.

It can be noted that Georgia is the odd one out, as it has no guidelines or legislature for what should be included in the breach notification.

California is, without a doubt, the strictest. The only optional elements as seen in the table are what the company is doing to protect the individual and the steps the individual should take to stay protected. On top, the legislature even mentions that they are optional and recommends including them. Adding on the formatting requirements as mentioned earlier, California is a shining example for other legislations to follow.

Table 1: Differences of breach notification content between sectors

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Required | Canada Public | BC Private | Alberta Private | California Private | Georgia Private | HIPAA |
| Nature and extent of breach | Y | Y | Y | Y | N | Y |
| Day or period breach occurred | Y | Y | Y | Y | N | Y |
| If risk notification delayed as result of investigation | N | N | N | Y | N | N |
| Type of personal information involved | Y | Y | Y | Y | N | Y |
| What company is doing to protect the individual or to investigate breach | Y | Y | Y | N | N | Y |
| Steps individual should take to reduce risk | Y | Y | N | N | N | Y |
| Contact info for business | Y | Y | Y | Y | N | Y |
| Contact info of major credit reporting agencies (under certain circumstances) | N | N | N | Y | N | N |
| Free offer for credit monitoring/ID theft prevention for at least 12 months in certain circumstances. | N | N | N | Y | N | N |

# New Canada Mandatory Breach Notification Law

Starting November 1, 2018, regulations for mandatory breach notification will apply across Canada. Companies covered under federal law will be required to report breaches to customers, affected third parties, and the federal privacy commissioner without unreasonable delay (Howard Solomon, 2018, para. 1).

With the new regulations, Howard Solomon (2018) writes the following about company responsibilities:

Under the data breach notification obligations companies must determine if the breach poses a “real risk of significant harm” to any individual whose information was involved in the breach by conducting a risk assessment. The assessment of risk must consider the sensitivity of the information involved, and the probability that the information will be misused. The law defines significant harm to include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss and identity theft. When the organization considers that a breach is posing a real risk of significant harm, it must notify affected individuals and report to the Privacy Commissioner of Canada as soon as feasible;

The company must notify any other organization that may be able to mitigate harm to affected individuals (para. 9).

Howard Solomon (2018) also writes about the content requirements for breach notifications:

The notification to affected individuals must include the following details:

* A description of the circumstances of the breach
* The day on which, or period during which, the breach occurred
* A description of the personal information that is the subject of the breach
* A description of the steps that the organization has taken to reduce the risk of harm to the affected individual resulting from the breach or to mitigate that harm
* a description of the steps that the affected individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm
* A toll-free number or email address that the affected individual can use to obtain further information about the breach
* Information about the organization’s internal complaint process and about the affected individual’s right, under the Act, to file a complaint with the Commissioner. (para 17).

The new federal breach notification law is expected to make a lasting impact on customer rights and privacy. Many hope the United States will follow suit next with its own federal mandatory breach notification law.

# Conclusions and Outlook

It won’t be long until it will become hard to imagine a time where privacy breach notifications were not mandatory. In recent years and in the near future, more and more legislatures are improving their privacy breach laws. In fact, many of the laws mentioned in this document were recent additions to legislature within the last 5 years. Privacy breach laws are becoming stricter to match the increasing amount of devastating privacy breaches.

The major problems discovered were privacy breach laws being too confusing and punishments not being tough enough. Regarding being confusing, a big example is the United States not having federal legislature regarding privacy breach notifications for federal institutions and private sector companies. It is currently a mish-mash between conflicting state laws and legislations only for specific industries, such as telecommunications. Thankfully, Canada is now tackling this issue with their own mandatory breach notification legislation, coming into effect on November 1, 2018. Punishments will also need to be heightened to prevent situations like the Equifax breach delay or the Uber breach cover up.

Many expect that the future of data privacy will be vastly different, however. In fact, many believe we are entering the data breach era. Tsian Gonen from NetworkWorld (2012) agrees saying, “Stop pretending you can prevent a perimeter breach. Accept that it will happen and build your security strategy accordingly.” (para. 8). Could we potentially see a law where all personal data must be encrypted? While great progress is being made on current privacy breach legislature, one may wonder whether the progress is truly in line with where we are heading.

# References

California Health and Safety Code Section 1280.15. (n.d.). Retrieved October 28, 2018, from <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC§ionNum=1280.15>

Centers for Medicare & Medicaid Services. (2016, August). HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES. Retrieved from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf>

Elkins, G. (n.d.). When Does the Law Require Companies like Equifax to Disclose Their Data Breaches? Retrieved from <http://elkinsplc.com/when-does-the-law-require-companies-like-equifax-to-disclose-their-data-breaches/>

Gonen, T. (2012, October 29). Breach prevention is dead. Long live the 'secure breach'. Retrieved from <https://www.networkworld.com/article/2161056/tech-primers/breach-prevention-is-dead--long-live-the--secure-breach-.html>

Gonzalez, G. (2018, February 14). Congress urged to adopt national data breach standard. Retrieved from <https://www.businessinsurance.com/article/20180214/NEWS06/912319215/Congress-urged-to-adopt-national-data-breach-standard>

Guidelines for Privacy Breaches. (2017, August 24). Retrieved October 25, 2018, from <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154>

HHS Office of the Secretary,Office for Civil Rights, & OCR. (2013, July 26). Breach Notification Rule. Retrieved October 28, 2018, from <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

Humiston, D. (2017, December 15). Will Your State's Privacy Law Be Superseded by HIPAA? Retrieved from <https://www.managedcaremag.com/archives/2002/5/will-your-states-privacy-law-be-superseded-hipaa>

Milkovich, D. (2018, June 07). 12 Alarming Cyber Security Facts and Stats | Cybint. Retrieved from <https://www.cybintsolutions.com/cyber-security-facts-stats/>

Newfoundland. (n.d.). Personal Health Information Act. Retrieved October 28, 2018, from <https://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm>

NueMD. (n.d.). California - Cal. Civ. Code §§ 1798.29, 1798.80 et seq. Retrieved October 28, 2018, from <https://www.nuemd.com/hipaa/breach-guide/CA.html>

Office of the Information and Privacy Commissioner of Alberta. (n.d.). How to Report a Privacy Breach. Retrieved October 28, 2018, from <https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx>

Office of the Privacy Commissioner of Canada. (2018, January 31). Summary of privacy laws in Canada. Retrieved October 28, 2018, from [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02\_05\_d\_15/#heading-0-0-3-1](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/%23heading-0-0-3-1)

Officer of the Information & Privacy Commissioner for British Columbia. (2012, March). Privacy Breaches: Tools and Resources. Retrieved October 27, 2018, from <https://www.oipc.bc.ca/guidance-documents/1428>

Ontario. (n.d.). Personal Health Information Protection Act. Retrieved October 28, 2018, from [https://www.ontario.ca/laws/statute/04p03#BK17](https://www.ontario.ca/laws/statute/04p03%23BK17)

SECURITY BREACH NOTIFICATION CHART - Georgia. (n.d.). Retrieved October 28, 2018, from <https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart-georgia.html>

Solomon, H. (2018, April 4). Canadian mandatory breach notification starts November 1, no regulations yet. Retrieved from <https://www.itworldcanada.com/article/canadian-mandatory-breach-notification-starts-november-1-no-regulations-yet/403558>

State Data Breach Law Summary. (2018, July). Retrieved October 25, 2018, from [https://www.bakerlaw.com/files/Uploads/Documents/Data Breach documents/State\_Data\_Breach\_Statute\_Form.pdf](https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf)