Advice from

THE BATTLEFRONT

Insight from life in the trenches

Ian S. Scarlett
416.746.4710
iscarlett@loonix.com

Ian S. Scarlett publishes as TheMidMarketLawyer.com and has been practising mid-market business law on the front line for more than two decades at Loopstra Nixon LLP. Ian has experience in advising clients in a broad range of industries across Canada as well as assisting foreign companies on their inbound Canadian legal needs. Ian is the former Managing Partner and is currently on the Executive Committee of the firm. More information on Ian is available at themidmarketlawyer.com including previous issues of ***The Battlefront***.

Disclosure Disclosure – *Show Me The Breaches!*

Data privacy is a sensitive subject in today's marketplace. Large retailers and governments have endured the public backlash of having to reluctantly announce breaches of security that have led to unauthorized disclosure of highly personal information. Brand reputation and corporate value can take immediate, and potentially long term, hits if an organization gains a reputation of lax security. Companies would prefer to handle breaches quietly and without public disclosure or scrutiny. However, changes are coming that will limit a company's ability to keep such breaches confidential.

This edition of ***The Battlefront*** reviews the recent regulatory changes by the Canadian government to force companies to advise both the government and affected individuals whenever personal private information is disclosed as a result of a breach in security.

The Legal Framework

In April 2000, the *Personal Information Protection and Electronics Documents Act* (PIPEDA) became law in Canada. Its dual purpose is the govern the collection, use and disclosure of personal information in commercial activities by the private sector as well as to promote confidence in electronic commerce. This regulatory scheme has been viewed by the European Union as adequate protection of personal information and has permitted the free flow of personal information from the EU to Canadian companies to foster increased trade.

In June 2015, the *Digital Privacy Act* (DPA) was enacted in Canada which made a number of amendments to PIPEDA. However, certain key changes (mandatory breach reporting and record-keeping) were delayed until a later date to be decided by the federal government.

Then, in May 2018, the new EU General Data Protection Regulation (GDPR) came into effect which significantly raised the standards and procedures related to protecting the personal information of EU citizens. In response, the Canadian government has now set the new Canadian obligations under DPA and PIPEDA to come into effect on November 1, 2018. This represents the new norm of protection obligations for the use of personal information in commercial activities.

The Changes

As of November 1, 2018, private companies in Ontario will have to comply with the following new obligations related to any breach of security safeguards that creates a real risk of significant harm:

(1) Notification to the Privacy Commissioner – This must include: (i) the circumstances and cause of the breach; (ii) the date(s) during which the breach occurred; (iii) the personal information disclosed; (iv) the number of affected individuals; (v) the steps taken to reduce or mitigate harm to affected individuals; (vi) the steps taken to notify affected individuals; and (vii) the name and contact information of the person who can speak for the company. The Commissioner has the authority to publish any information relating to the breach if it would be in the public interest to do so.

(2) Notification to Affected Individuals – This notice must include sufficient information such that the individuals understand the significance of the breach and how they may take steps to reduce their risk of harm. The notice must be given directly to the affected individuals "*in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances*". This provides some flexibility to design a procedure that is appropriate for the business. Indirect notification (ex: posting notice to a website) may be permissible if: (i) direct notification would be likely to cause further harm; (ii) direct notification would be likely to cause undue hardship for the company; or (iii) the company does not have the contact information for the affected individual. A reasonable procedure may include multiple distribution channels (ex: mail and website).

(3) Notification to Other Organizations – The company may also be required to give notice to other companies or governmental institutions if such notice could reduce the risk of harm.

(4) Record-keeping of all breaches – Companies must keep records of every breach of their safeguards involving personal information under their control and their actions in response of each breach. This information must be kept for 24 months in a "breach file" that details each breach. There is no threshold on the extent of a breach or the information disclosed. All breaches must be recorded even if the breach did not trigger the obligation to notify the Commissioner or any individual.

These new obligations are mandatory and contraventions carry fines of up to $100,000. In addition, any failure to establish security safeguards is deemed to be a breach of these obligations.

What is a Reportable Breach?

The obligation to report is triggered when it is reasonable to believe that the breach creates "*a real risk of significant harm to the individual*". This definition hinges on "*significant harm*" and "*real risk*".

"***Significant harm***" is a broad concept which includes, among other things, humiliation, damage to reputation or relationships, loss of employment, business or professional activities, financial loss and identity theft. However, this is an open-ended definition that potentially could capture other forms of harms as well, even harms not currently considered to be related to unauthorized disclosure of personal information.

"***Real risk***" is a more subjective concept that requires the company to consider the sensitivity of the information and the probability the information can be misused. There is no bright line rule or guidance that can distinguish a real risk from a theoretical possibility. The company must carefully consider how the disclosed information could be used that may lead to significant harm.

If a breach has created "***a real risk of significant harm to the individual***", the reporting obligations are triggered. The company must provide notice to the Commissioner in a form specified by the Commissioner. The company must also provide notice to affected individuals "***as soon as feasible***" after it is determined the breach has occurred. The content of this notice is not defined as it depends upon the nature of the breach. The company must give the affected information the information necessary so that they may minimize their personal risk.

The Results

In addition to the additional administrative effort required to maintain a "breach file", there are various other collateral impacts that may arise as a result of this regulatory change. Likely issues include:

(1) **When to Report** - There is no clear, bright line definition of what is, or is not, a security breach that would trigger the obligation to notify the Commissioner and the affected individuals. Companies must carefully consider all the factors of the breach when deciding whether the reporting obligations are triggered. However, even a carefully reached decision *not to report* may not be an adequate defence. The Commissioner may take a

different view and seek to enforce penalties if the breach subsequently comes to the attention of the Commissioner.

(2) **Forced Disclosure** – PIPEDA gives the Commissioner the authority to require any company to provide a copy of its security breach record. There is no threshold as to when such a request can be made; the Commissioner may require a copy at any time. The Commissioner may also publish any of such information or commence an audit to investigate breaches further. This could lead to penalties if the Commissioner subsequently determines records are incomplete or a security breach was not reported at the appropriate time. Additionally, once this information is with the Commissioner, conceptually it could become subject to a *Access to Information Act* request by the public (i.e. news media) which could lead to widescale disclosure of the breach incident.

(3) **Outside Service Providers** - Companies who use outside service providers to process personal information (ex: payroll service providers) may have to disclose breaches involving the personal information they made available to their service providers. However, the service provider may not have a similar reporting obligation if the service provider is not controlling the personal information as contemplated by PIPEDA. Companies must carefully ensure the service contract requires the service provider to also provide the information necessary such that the company can comply with its PIPEDA obligations.

(4) **Future Litigation** - The record-keeping requirement may also become fodder in any litigation related to alleged security breaches, particularly any class action litigation. Litigators will certainly request copies of the company's "breach file" in an attempt to easily get information on the company's knowledge at the time of the alleged events. It would also likely to presume that affected individuals would complain to the Commissioner who in turn would request a copy of such "breach file" to conduct an audit. Any attempt by a company to not record breach information to insulate it from litigation would likely increase its risk of action by the Commissioner.

(5) **Impact on Insurance** - Insurance companies may also request a copy of a company "breach file" when considering insurance premiums and renewals. This will likely affect a company's risk profile, any insurer's decision on offering insurance, and also setting the insurance costs. Companies will minimal breaches likely will easily find insurance at a reasonable cost, while companies with more security breaches may face higher insurance costs, or perhaps even becoming unable to find insurance, particularly cyber liability insurance. Failing to obtain insurance renewals could trigger collateral problems with office leases, bank financing, mortgages, etc.

(6) **Encryption may not be enough** – While encrypting data may be a prudent measure, encryption alone may not be sufficient to satisfy these new obligations. The company must assess the overall situation as to how it handles and processes personal information in deciding whether encryption is sufficient. If it subsequently turns out that the encryption can be broken by determined hackers, then the company may be at risk of a security breach. Companies must take a broader view of security safeguards other than just encryption.

Thoughts to Take Away

The days of handling suspected security breaches quietly and without governmental involvement or public scrutiny may be coming to an end on November 1, 2018. Companies must comply with the new "breach file" requirements and be prepared to take the specific courses of action when a breach occurs.

Dealing with a security breach can create havoc and uncertainty within the company, including senior management who must grapple not only with understanding the extent of the breach; how to immediately stop any further such breaches; how to deal with managing the public message; but now must also carefully consider if and when to report to the Privacy Commissioner and notify affected individuals. This can present an overwhelming myriad of conflicting interests and obligations to be quickly balanced in a stressful time.

The better approach is for companies to prepare a breach procedure whereby the obligations and responsibilities are assigned to specific individuals to handle when a breach occurs. This battleplan permits all involved individuals to understand their roles and scope of authority in these events. A coordinated approach will make the best out of a bad situation and permit the company not only to comply with the new obligations under PIPEDA, but also demonstrate to the public that it respects the sensitivity of its customers regarding their personal information.

Electronic commerce is steadily increasing and is a vital component to today's economy. Personal information is a key to successful electronic commerce, but comes with new obligations to securely protect such a valuable asset. Security should always be paramount, but when a breach occurs, companies be prepared to comply with the new obligations of ***disclosure disclosure***!

About Loopstra Nixon LLP

Loopstra Nixon is a full-service Canadian business and public law firm dedicated to serving clients involved in business and finance, litigation and dispute resolution, municipal, land use planning and development, and commercial real estate. Major financial institutions, insurance companies, municipal governments, and real estate developers along with corporate organizations and individuals are among the wide range of clients we are proud to serve.

About ***The Battlefront***

This article contains general information only. ***The Battlefront*** is a brief canvasing of the topic presented and should not be relied upon as professional advice in making any personal or business decisions. Always consult with a licenced legal professional before making any decisions regarding your own personal or business needs. The author takes no responsibility to update any of the information presented in this article.