FTR Now

Federal Government Introduces Legislation to Create “PIPEDA 2.0”

Date: June 9, 2010

On May 25th, the federal government introduced Bill C-29, the *Safeguarding Canadians’ Personal Information Act*, and Bill C-28, the *Fighting Internet and Wireless Spam Act*. If passed, these Bills would make changes to the *Personal Information Protection and Electronic Documents Act* (“*PIPEDA*” or the “*Act*”) that are of significance to federal sector employers, as well as organizations that collect, use, and disclose personal information in the course of their commercial operations.

Bill C-29 would make long-awaited amendments to *PIPEDA* to address perceived weaknesses and ambiguities that have been part of the *Act* since its inception. Bill C-29 would also enact new data breach reporting and notification duties.

Bill C-28 would enact comprehensive anti-SPAM legislation that would exist independently of *PIPEDA*, and would create a private right of action for non-compliance with the new anti-SPAM legislation and for non-compliance with proposed complementary provisions in *PIPEDA*.

In this *FTR Now*, we summarize the major changes to *PIPEDA* introduced by the two Bills, and explain why these changes make it time for Canadian organizations to pay special attention to privacy protection and data security.

NEW DATA BREACH REPORTING AND NOTIFICATION DUTIES

Bill C-29 would impose data breach reporting and notification duties on organizations by creating three separate duties:

- a duty to report all “material” breaches of security safeguards involving personal information under their control to the Privacy Commissioner;
- a duty to notify individuals of any breach of security safeguards involving personal information under their control when “reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual”; and
- in the same circumstances, a duty to notify other organizations or institutions if they may be able to reduce the risk of harm that could result from the breach or mitigate that harm.

Organizations will be required to give notification “as soon as feasible” after confirming the breach and concluding that notification is required. Bill C-29 includes factors to assist organizations in

assessing the materiality and risk profile of a breach. Though organizations must report material breaches to the Commissioner, she does not have the power to order notification to individuals.

NEW EMPLOYMENT ADMINISTRATION EXCEPTION

Bill C-29 would create a new employment exception to the *PIPEDA* consent rule. In short, federal sector employers would be able to collect, use and disclose personal information, without consent, in the course of establishing, managing or terminating employment relationships. The focus of regulation regarding employees would be redirected from consent to focus on whether the collection, use and disclosure of employee personal information was “necessary” and whether proper notification to employees was provided.

LIMITATIONS ON PROTECTION OF BUSINESS CONTACT AND WORK PRODUCT INFORMATION

Bill C-29 would enact new provisions to limit the protection given to so-called “business contact information” and “work product information.”

“Business contact information” would become a defined term, meaning an individual’s “name, position name or title, work address, work telephone number, work facsimile number, work electronic mail address and any similar information.” This information would not be protected. Significantly, business e-mail addresses and business facsimile numbers would be excluded from the scope of *PIPEDA* protection, which is not currently the case.

Bill C-29 would also enact a series of new provisions to create an exception to the consent rule for “work product information” – information produced by individuals in the course of employment, business or professional practice. This information could be collected, used and disclosed without consent provided that the collection, use or disclosure was consistent with the purpose for which the information was produced. The more flexible “consistent purpose” requirement is common to many public sector privacy protection statutes.

NEW BUSINESS TRANSACTION EXCEPTION

Bill C-29 would create a new exception to facilitate the disclosure and use of personal information in the course of entering into and concluding a business transaction and, following the closing of a transaction, ceding control of a business operation.

Parties to a transaction would be able to disclose and use personal information without consent provided that such disclosure and use was a necessary part of due diligence or was necessary to complete the transaction, and provided that they entered a data protection agreement that met certain requirements. Parties who successfully completed a transaction would be able to use and

disclose the same personal information provided that such use and disclosure was necessary for carrying on the business or activity that was the object of the transaction, and provided that notification to individuals was given within a reasonable time after the transaction was completed and provided that they entered a data protection agreement that met certain requirements.

Bill C-29 would also impose a statutory duty to comply with a data protection agreement that had been entered into to take advantage of the new business transaction exception.

NEW ARTICULATION OF INFORMED CONSENT REQUIREMENT

Bill C-29 would also enact a provision that specifies the requirements for informed consent. The consent of an individual would only be valid “if it is reasonable to expect that the individual understands the nature, purpose and consequence of the collection, use or disclosure of personal information to which they are consenting.”

DISCLOSURE EXCEPTIONS MODIFIED

Bill C-29 would make a number of changes to the exceptions for disclosures that could be made without consent.

PIPEDA would specify that organizations could disclose personal information to respond to bona fide law enforcement requests, even if such requests were not based on a warrant, subpoena or production order. It would also permit the disclosure of personal information to other organizations (and not just investigative bodies) where necessary to investigate a breach of an agreement or a contravention of law and to prevent, detect or suppress fraud in certain circumstances.

ANTI-SPAM LEGISLATION AND A NEW PRIVATE RIGHT OF ACTION

The main purpose of Bill C-28 is to enact comprehensive anti-SPAM legislation (the *Fighting Internet and Wireless Spam Act*) to regulate, among other things, the sending of commercial electronic messages without consent, the alteration of electronic data transmissions and the unauthorized installation of computer programs.

Bill C-28 would also make complementary amendments to *PIPEDA*, including prescribing rules related to the collection of an individual’s electronic address (including e-mail and instant messaging accounts) and the illegal collection and use of personal information from an individual’s computer.

As part of these changes, Bill C-28 would created a new private right of action for the contravention of the new anti-SPAM legislation created by the Bill or for the contravention of the complementary amendments to *PIPEDA*.

PRIVACY PROTECTION AND DATA SECURITY ARE ABOUT TO BECOME EVEN MORE CRITICAL IN CANADA

Many of the proposed substantive amendments to *PIPEDA* are changes that would be welcome to organizations regulated by the *Act* as they clarify ambiguities and address practical issues not contemplated by the original legislation.

Some may argue that *PIPEDA* has been a “paper tiger” since it came into force. Very few organizations subject to the *Act* have been compelled to answer a *PIPEDA* complaint, and far fewer have had to respond to a *PIPEDA* application in the Federal Court. Some have compared *PIPEDA*’s status to that of provincial and federal human rights legislation, but it has not given rise to nearly the same impact nor has it been the source of the same degree of operational risk.

Bills C-29 and C-28 could change this. Though the administrative procedure for handling *PIPEDA* complaints would largely remain the same – indeed, the Commissioner would actually be granted a greater discretion to decline to deal with complaints – the new data breach reporting and notification duties should cause organizations to engage with individuals about matters regulated by *PIPEDA* in a manner that many have not yet done. This engagement would come with the significant costs of notification. Even more significantly, it would come post-breach, when organizations are vulnerable and large groups of individuals are upset.

Organizations should think about engaging with individuals proactively, before a breach occurs. This includes implementing systems and processes that would allow them to confidently answer the questions that might be asked by individuals who are notified of a data breach. Organizations who can answer those questions may be able to disarm aggravated individuals and avoid, or at least reduce, conflict.

We will follow the progress of these Bills as they proceed through the legislative process. If you have any questions please contact Dan Michaluk at 416.864.7253, Paul Broad at 519.931.5604, or our colleague Scott Williams at 416.864.7325