Bloomberg Law®

INSIGHT: Canada's New Breach Notification Law—A Global Reach?

By Craig Newman and Stephanie Teplin
November 30, 2018

Patterson Belknap attorneys Craig A. Newman and Stephanie Teplin warn that Canada's new data breach notification regulation is surprisingly expansive and say U.S. business with connections to Canada need to assess whether they are subject to the rules based on the extent of their relationship with Canada, its businesses, and citizens.

The patchwork of data privacy laws—both within the U.S. and abroad—has always posed challenges for multinational businesses. But Canada has enacted a new breach notification regulation that is surprisingly expansive and any U.S. business with a connection to Canada--- no matter how remote --- needs to know it took effect Nov. 1 and keep an eye on it.

The new Canadian privacy laws are intended to bring the country in line with the European Union's General Data Protection Regulation (GDPR), which has been in effect for almost six months.

Multi-jurisdictional Reach

No matter where located, businesses with a connection to Canada will need to know the law's requirements, particularly if they have Canadian customers, come into contact with Canadians' personal data, or direct their services or advertising into Canada.

A Canadian court and the Office of the Privacy Commissioner (OPC or Privacy Commissioner) have already recognized these as sufficient contacts to bring a company within the scope of Canada's data privacy laws. Once triggered, the new provisions in the Personal Information Protection and Electronic Documents Act (PIPEDA) dictate a set of requirements including mandatory breach notification and tracking of data breaches.

The jurisdictional limitations of Canada's data security laws were established in a 2007 case, Lawson v. Accusearch Inc., 4 F.C.R. 314 (Fed. Ct. 2007). In Lawson, a Canadian citizen and law professor became concerned that Accusearch Inc., a Wyoming-based company offering background checks, was misusing Canadians' data. She ordered a background check on herself, and after receiving it and confirming that it must have relied on Canadian data, filed a complaint with the OPC. The Privacy Commissioner declined to investigate on jurisdictional grounds, but the court reversed, noting that a connection to the jurisdiction had been sufficiently established because "much of the data had to have come from Canada."

Following this principle, the Privacy Commissioner has exercised its regulatory power to investigate the activities of a number of non-Canadian companies for potential privacy violations. Last spring, the OPC released a report of an investigation into Profile Technology Ltd., a New Zealand-based company, that allegedly copied and retained Canadian Facebook users' information without consent to index it for search engine use, and later, to establish its own social networking site. PIPEDA Report of Findings #2018-002.

Although Profile Technology argued that the Privacy Commissioner should decline to exercise jurisdiction and refer the investigation to its New Zealand counterpart, it found a "real and substantial connection" with Canada based on the fact that the website had information for millions of Canadian users, allowed searches to be limited to Canadians, and delivered Canadian-based advertising.

The Privacy Commissioner also concluded that complaints against a Romanian business that republished Canadian court decisions involving Canadian individuals were well-founded, after identifying "several indicial of a real and substantial link to Canada." PIPEDA Report of Findings #2015-002.

Effects of Canadian Breach Notification Law

The new Breach of Security Safeguards Regulations implement certain provisions of the Digital Privacy Act, which amended PIPEDA, Canada's federal privacy law. The new regulations, which went into effect on November 1, 2018, require organizations to report a data breach—

even if only one person is affected—if it creates a "real risk of significant harm."

Under PIPEDA, that can mean "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." An assessment of risk must include evaluation of the sensitivity of the information, as well as the possibility for misuse.

The new regulations require a breach notice be sent to the OPC, and include a description of the steps the organization is taking to reduce the risk of harm to affected individuals. And notice must be given to the affected individuals themselves "in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances."

According to official guidance released by the Privacy Commissioner, notice must include "enough information to allow the individual to understand the significance of the breach of security safeguards to them and to take steps, if any are possible, to reduce the risk of harm that could result from the breach or mitigate the harm." Notification to other organizations—including law enforcement—may be required as well, if those outside organizations could assist in mitigating the harm to affected individuals. The Canadian law does not set a specific time frame to report a breach but requires that notice be given as soon as feasible.

It also imposes a two-year record retention requirement.

The cost of noncompliance with the Canadian law is steep. If a business knowingly withholds information about a breach or fails to keep the required records, fines can reach C$100,000 per day (roughly $132,500 U.S.). While the Privacy Commissioner cannot itself prosecute offenses or impose fines, it can refer violations to the Attorney General of Canada for prosecution.

The Patchwork Problem

While the Canadian regulation is intended to bring that country's laws in line with the GDPR, it may exacerbate the problem of patchwork regulation for multi-national companies that regularly come into contact with Canadian personal data.

The Canadian legislature even recognized the fragmented nature of its own privacy laws and exempted organizations and activities that take place wholly within the Canadian provinces of Quebec, British Columbia and Alberta, which all have laws that were deemed similar to PIPEDA. But there is no such carve-out for companies that are already regulated by a U.S. privacy law, such as California's new Consumer Privacy Act of 2018.

The enactment of new Canadian breach notification rules may make the problem of patchwork regulation more acute for multinational organizations that deal with the personal data of Canadians. Such companies should carefully assess whether they are subject to the law based on the extent of their relationship with Canada, its businesses and citizens.

Craig A. Newman, a partner at Patterson Belknap Webb & Tyler LLP in New York and chair of the firm's data security and privacy practice, represents public and private companies, their boards and leadership teams in data security matters, internal investigations, litigation, corporate governance, compliance and crisis communications.

Stephanie Teplin, an associate at Patterson Belknap in New York, served as a law clerk to the Honorable John M. Walker Jr. of the U.S. Court of Appeals for the Second Circuit.