FTR Nexus

Setting up Shop in Canada? What U.S. Employers Need to Know About Canadian Privacy Law

Date: December 15, 2017

While Canada and the United States are alike in many respects, there are a few key differences in privacy law that U.S. organizations should be aware of if you are considering buying, selling or operating a business in Canada.

Two Canadian Privacy Issues That May Surprise You

1. Think Twice Before You Press “Send”

The compliance obligations under Canada’s anti-spam law, known as “CASL”, are onerous. Unlike the “opt-out” model that is the basis of United States law, under CASL express consent is the default requirement. Penalties for non-compliance with CASL are severe: a corporation could be fined up to $10 million per violation.

What you need to know:

- CASL came into force in 2014 (with some exceptions) and restricts the sending of Commercial Electronic Messages (CEMs). Generally, an email message is a CEM where one of its purposes is to encourage the recipient to participate in commercial activity.
- Subject to certain exceptions, CASL prohibits:
    - sending, or causing or permitting to be sent, CEMs without the express or implied consent of the recipient and in compliance with prescribed form and content;
    - altering transmission data in an electronic message so that it is delivered to an alternate address without express consent, unless the alteration is in accordance with a court order; and
    - installing a computer program on another’s computer, or causing an electronic message to be sent from such a computer, again without express consent, unless this is done in compliance with a court order.
- Consent must be obtained when sending a CEM to an electronic address. In addition to this, the CEM must set out certain information and an unsubscribe mechanism.
- CASL imposes severe penalties for non-compliance. The maximum penalty per violation is set at $1 million for an individual and at $10 million for a corporation.
- Directors, officers and other employees can be vicariously liable for incidents of non-compliance

- The Canadian Radio-television and Telecommunications Commission (CRTC) has been given broad powers of enforcement.
- The coming into force of a private right of action under CASL has been delayed indefinitely in light of concerns raised by various parties. That right of action would allow an individual to rely on an unsolicited CEM as the foundation for a civil action.

So what is a U.S. organization to do?

Very simply, maintain a separate data base for Canadian addresses and manage it in accordance with Canadian law. Compliance with United States anti-spam law will generally not meet Canadian requirements.

2. New Data Breach Obligations Are Coming Soon

Recent data breach security amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will create significant new compliance obligations for federally regulated employers and organizations that handle personal information in the course of commercial activity. The changes will likely give rise to additional costs and subject organizations to an increased risk of litigation, including data breach class actions. (Note that these amendments have been passed, but are not yet in force.)

Organizations will now be required to comply with mandatory requirements regarding a “breach of security safeguards.” That term is defined as “the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization’s security safeguards.” The requirements are set out below:

- Organizations must report a breach of security safeguards to the Office of the Privacy Commissioner of Canada (the OPC) if it is reasonable to believe the breach creates a real risk of significant harm to an individual.
- Unless prohibited by law, organizations must notify affected individuals of a breach of security safeguards if it creates a real risk of significant harm.
  The notification must contain sufficient information to allow individuals to understand the impact of the breach and to allow them to take steps to reduce or mitigate the risk of harm that may result, and any other prescribed information. The notification must be conspicuous and given directly, or where prescribed, indirectly to the individual.
- If notification to individuals is made, organizations must also notify other organizations if they believe those other organizations may be able to reduce the risk of harm or mitigate that harm or if any of the prescribed conditions are met.
- Organizations must keep and maintain a record of every breach of security safeguards for provision to the OPC on request.
  Note that this recordkeeping requirement is not limited by the requirement that a “real risk of significant harm” may result, thereby creating the requirement that ***every*** breach of

security safeguards, no matter how insignificant or harmless, must be recorded.

Factors relevant to determining whether a breach of data security creates a “real risk” are set out in the legislation, and include:

a. the sensitivity of the personal information involved;
b. the probability that the personal information has been, is being or will be misused; and
c. any other prescribed factor.

“Significant harm” includes “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.” (s. 10.1(7)).

The supporting regulations to the PIPEDA amendments will flesh out the specific requirements imposed on organizations. Once they are in place, the amendments will be proclaimed into force. Proposed regulations were published on September 2, 2017 and are awaiting finalization.

Organizations must take steps now to prepare for these new requirements. Those without formal incident response policies should act to formalize and document their incident response processes. Organizations with formal incident response policies should update them as soon as the government finalizes the regulation that will detail the reporting and recordkeeping requirements. All organizations should address the new recordkeeping requirement with an understanding that “the incident record” has the potential to be key evidence in many regulatory matters and civil disputes.
