

Canada's anti-spam legislation (CASL) will have a significant impact on the electronic communication practices of companies operating in the Canadian marketplace when it comes into force. Designed as one of the most stringent anti-spam regimes in the world, the legislation imposes significant restrictions on the use of electronic messages that include not only email but also text messages, instant messages and other messages sent from similar accounts (likely including some forms of social media messaging) for commercial purposes.

CASL will apply if the electronic message is a "commercial electronic message" (CEM). However, such messages merely need to encourage participation in conduct of a commercial character, whether or not there is an expectation of profit, to be caught by CASL. Under CASL, unless specifically permitted by the legislation, the recipient of the CEM must have consented to receiving the CEM before it was sent. This is referred to as an "opt-in" system and differs from an "opt-out" system with which companies operating in the U.S., and some other international jurisdictions, may be familiar. It is worth noting that an electronic message requesting consent to receive further CEMs is itself a CEM and, therefore, cannot be sent without the consent of the recipient. Each CEM must meet several form and content requirements. Among other things, each CEM must provide an unsubscribe mechanism whereby recipients can indicate that they do not consent to receiving any further messages. There are substantial administrative monetary penalties available under the act as well as a private right of action that will allow any person who believes they have been affected by a breach of CASL to apply to the court to seek redress. Once in force, plaintiffs' counsel are likely to consider bringing anti-spam class actions.

It is not entirely clear when CASL will be proclaimed into force as there have been significant delays in the publication and finalization of the regulations under the legislation. In light of concerns raised in submissions filed with Industry Canada and the Canadian Radio-television Telecommunications Commission during the public comment period on the draft regulations that were published in early fall of 2011, it appears likely that there will be an additional public consultation period in the summer of 2012 for a revised set of regulations to be published by Industry Canada. As a result, the legislation is unlikely to come into force before the end of 2012. The regulators have stated that some interpretation bulletins or guidelines will be issued prior to the legislation coming into force.

Given the significant impact that this legislation is likely to have on many businesses operating in the Canadian marketplace and the ambiguities that have thus far plagued its implementation, organizations should keep the progress of this legislation on their radar as 2012 proceeds.

For more information, please see the Blakes CASL microsite at <http://www.blakes.com/english/antispam.asp>.

BILL C-12: AN ACT TO AMEND THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Recently proposed amendments to PIPEDA will be of interest to Canadian businesses as they both clarify the application of the legislation in some circumstances as well as impose new obligations in others. These amendments were introduced in Bill C-12 by the federal government on September 29, 2011.

Among other things, Bill C-12 excludes "business contact information" (which is defined to include an individual's name, position name or title, work address, work telephone number, work facsimile number, work electronic mail address and any similar information about the individual) from the requirements under PIPEDA if the information is collected, used or disclosed solely for the purpose of communicating with that individual regarding their employment, business or profession. Another key amendment permits organizations to use and disclose personal information without the knowledge or consent of an individual if the information is necessary to determine whether to proceed with or complete a prospective "business transaction." This exception does not apply to business transactions for the primary purpose of exchanging personal information.

Bill C-12 also introduces new data breach notification requirements that have some similarities with, but are by no means identical to, the mandatory reporting requirements that were introduced into Alberta privacy legislation in 2010. Organizations must report material breaches of security safeguards involving personal information under their control to the Privacy Commissioner and notify the affected individuals of any breaches if it is reasonable to believe that the breaches create a "real risk of significant harm" to the individuals. Organizations may also have to notify other organizations or government institutions if doing so may reduce the risk of harm or mitigate the harm that may result. Bill C-12 is currently at the first reading stage in the House of Commons.

Continued on reverse

BEHAVIOURAL ADVERTISING GUIDELINES ISSUED BY FEDERAL PRIVACY COMMISSIONER

The federal Privacy Commissioner recently issued *Privacy and Online Behavioural Advertising guidelines*. Online behavioural advertising involves tracking consumers' online activities to collect information about their interests and activities in order to direct advertising targeted to those interests and activities. The guidelines identify that the Commissioner takes the view that information collected for online behavioural advertising will generally constitute personal information (i.e., "information about an identifiable individual"). As such, the requirement of PIPEDA that the individual must provide knowledgeable consent for the collection, use or disclosure of his or her personal information in online behavioural advertising applies.

The guidelines take the position that "opt-out" (i.e., implied) consent may be considered reasonable for non-sensitive personal information if several criteria are met, including that individuals are made aware of the practice in a clear and understandable manner; individuals are informed of the practices at the time of collection (including the various parties involved) and are easily able to opt out of the practice; the opt-out mechanism takes effect immediately and is persistent; and information is destroyed or de-identified as soon as possible. The guidelines state that if an individual is not able to decline the behavioural tracking by an opt-out mechanism or if opting out renders the service unusable then organizations should not use that type of technology for online behavioural advertising. In her blog post on December 16, 2011, regarding the new guidelines, the Commissioner warns that "in the months to come, we'll be watching the watchers to see that our guidance is being followed. And if we see troubling trends we'll take enforcement action."

RECENT CASE LAW ON PERSONAL INFORMATION LEGISLATION

Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner), 2011 ABCA 94

An Alberta furniture retailer's practice of recording driver's licences of persons picking up furniture was recently upheld when the Supreme Court of Canada dismissed the Alberta Information and Privacy Commissioner's request to appeal the ruling of the Court of Appeal of Alberta to overturn a decision of the Alberta Privacy Commissioner. The case related to Leon's policy of collecting driver's licence plate numbers in order to prevent fraud by individuals picking up furniture. The Court of Appeal held that driver's licence

numbers were personal information under the definition in Alberta's *Personal Information Protection Act* (PIPA) but that licence plate numbers were not as they were linked to a vehicle and not an individual. The Court of Appeal further held that collection of driver's licence numbers in the given circumstance for the purpose of preventing fraud was reasonable. The court highlighted that just because the Alberta Privacy Commissioner believed that there was a better or less privacy-intrusive way to prevent fraud did not mean that Leon's practice of collecting driver's licence numbers was unreasonable and therefore contrary to PIPA.

One of the key points highlighted in this case—that an organization is not required to implement the objectively least intrusive option available but rather that their practices must be reasonable—may be a valuable argument to organizations that are required to defend their personal information practices. The extent to which it will be applicable under the federal PIPEDA, however, remains to be seen.

APPLICATION OF ONTARIO FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA) EXTENDED TO INCLUDE HOSPITALS

Ontario hospitals are now subject to the Ontario public-sector legislation known as FIPPA, including provisions relating to requests from the public for access to records. These amendments came into force on January 1, 2012, and apply retrospectively to records that came into the custody or control of hospitals on or after January 1, 2007. Several types of hospital records will be exempt from disclosure under FIPPA, including ecclesiastical records, records that relate to the operations of a hospital foundation, administrative records of a member of a health profession, records relating to charitable donations, records relating to the provision of abortion services and records for teaching or research associated with a hospital. While these changes will not affect the regulation of personal health information privacy under existing Ontario personal health privacy legislation, the amendments may have implications for companies that enter into supply agreements or other contractual relationships with hospitals. As the Ontario Information and Privacy Commissioner has consistently held that third-party contracts with designated institutions are mutually negotiated, and not supplied by the third party, information contained within these contracts may be subject to disclosure pursuant to access to information requests.