PricewaterhouseCoopers LLP Midwest Privacy Retreat (November 2, 2016)
Canadian Privacy Law
Melissa Krasnow (with thanks to Andrea York at andrea.york@blakes.com)

Overview of Canadian privacy laws in the private sector
• Canada has a comprehensive federal private sector privacy statute and provincial private sector privacy statutes
• General principle: Consent to collect, use or disclose personal information is generally required (with certain exceptions)
• Also, the collecting, using and disclosing of that information must be for purposes that a reasonable person would consider appropriate in the circumstances, regardless of whether the individual has consented to the collection, use or disclosure of their personal information

Federal private sector privacy law: Personal Information Protection and Electronic Documents Act (PIPEDA)
• PIPEDA generally applies to all collection, use or disclosure of personal information by organizations in commercial activity
• PIPEDA defines personal information broadly, including any information about an identifiable individual, whether public or private, with certain exceptions
• PIPEDA does not apply to the collection, use and disclosure of employee information by provincially regulated private sector employers (i.e., most organizations)
• Federally regulated employers (e.g., banks, airlines, telecommunication companies, etc.) are covered, but most Canadian companies are provincially regulated
• Organizations are exempt from PIPEDA regarding activities covered by the substantially similar provincial laws

Canadian Bill S-4 (Digital Privacy Act) amends PIPEDA – provisions in force
• Individual consent is valid if it is reasonable to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which the individual is consenting
• Certain new exceptions to consent requirement
• "Business transaction" exemption: organizations can use and disclose personal information without consent in connection with mergers, acquisitions, financings, etc. (both during due diligence and post-closing) where certain conditions are met
• Business contact information is defined more broadly (includes business email addresses) and is not excluded from the definition of personal information. However, PIPEDA's personal information provisions will not apply to the collection, use and disclosure of business contact information by an organization solely for the purpose of communicating with an individual about their employment, business or profession
• Canadian Privacy Commissioner authority to enter into compliance agreements with organizations reasonably believed to have violated or that are about to violate PIPEDA

Canadian Bill S-4 (Digital Privacy Act) amends PIPEDA – provisions to come into force
• Mandatory breach notification to Canadian Privacy Commissioner, individuals and other organizations and government entities (see https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11177.html)
• Required organizational maintenance of record of each breach
• Monetary penalties for non-compliance

Comprehensive provincial private sector privacy laws
Alberta, British Columbia and Quebec have comprehensive private sector privacy laws
• Manitoba adopted a comprehensive private sector privacy law (unclear whether or when it will be proclaimed into force)
• Other provinces have more limited privacy legislation, for example, dealing with health information
• These provincial comprehensive sector privacy laws apply to organizations collecting, using or disclosing personal information within a province where the province has enacted legislation that is substantially similar to PIPEDA

Canadian private sector privacy laws addressing data breach notification
• Alberta – must notify Alberta Privacy Commissioner, which can direct notification to individuals
• Manitoba – must notify individuals (unclear whether or when it will be proclaimed into force)
• Canadian Privacy Commissioner – voluntary privacy breach guidelines
• Federal and provincial privacy commissioners have also published guidelines that suggest disclosure and notification should be made in certain circumstances

Canada's Anti-Spam Law (CASL)
• Effective July 1, 2014
• Applies to all commercial electronic messages (CEMs), including email, text messages, instant messages and social networking communications where the computer system used to send or access the CEM is located in Canada, unless the CEM is subject to an exception
• Cannot send a CEM unless the recipient consented to its receipt and the message meets certain form and content requirements
• Effective January 15, 2015 – cannot install computer programs on another person's computer without express prior consent

CASL enforcement/actions
• Significant administrative monetary penalties
• Liability for senders, those who cause sending and those who aid, induce or procure sending of prohibited CEMs
• Vicarious liability for directors, officers and employers for noncompliance with CASL, subject to a due diligence defense
• Effective July 1, 2017 – violation of CASL also can be the subject of a private right of action by any affected individual or organization