

SPAM AND PRIVACY UPDATE

Are you compliant?

SEMINAR WEDNESDAY, APRIL 13, 2011

SPAM AND PRIVACY UPDATE

Are you compliant?

CONTENTS

SPEAKERS

Wesley Ng
Partner
Stikeman Elliott

David Elder
Counsel
Stikeman Elliott

Karen Jackson
Partner
Stikeman Elliott

PRESENTATION SLIDES

The Wide Net of Canada's New Anti-Spam Legislation
David Elder

Canadian Privacy Law: Online Tracking and Recent Developments
Karen Jackson

ARTICLES

"Spam's big Hammer"
Andi Balla, *CanadianLawyermag.com*

"Time to take steps assuring compliance of new spam law"
Drew Hasselback, *Financial Post*

"Canadian anti-spam legislation on fast-track"
David Elder

"Anti-spam law governs software – not just email"
David Elder, *The Lawyers Weekly*

Additional Links

FIRM PROFILE

An overview of Stikeman Elliott and our Technology, Intellectual Property and Communications Groups

SPAM AND PRIVACY UPDATE

Are you compliant?

PROFILES OF TODAY'S SPEAKERS



Wesley Ng
Stikeman Elliott



David Elder
Stikeman Elliott



Karen Jackson
Stikeman Elliott

SEMINAR WEDNESDAY, APRIL 13, 2011



Wesley R. Ng

5300 Commerce Court West, 199 Bay Street, Toronto, Canada M5L 1B9
Direct: (416) 869-5218 Fax: (416) 947-0866 wng@stikeman.com

Law Practice

Wesley Ng is a partner in the Corporate Group of the Toronto office and a member of the firm's Technology Practice Group. Mr. Ng's practice focuses on information technology, e-commerce, and biotechnology transactions as well as privacy related matters. He has acted for financial institutions, public sector entities and global multi nationals in connection with global outsourcings, SAS/ASP arrangements and transformational procurements.

Mr. Ng has been responsible for the technology portions of acquisitions and outsourcing arrangements in numerous industries, including financial services, insurance, telecommunications, postal services, optical and wireless manufacturing and design, health care, municipal services, biotechnology and software development and maintenance. He has extensive experience advising both service providers and service recipients on outsourcing and technology transactions.

In addition, Mr. Ng regularly assists his clients with licensing, joint ventures, strategic partnerships, financing, online trading and technology development. He also regularly advises clients on privacy issues across numerous industries, including financial services, insurance, retail, manufacturing and distribution, ticketing services, energy and resources, pharmaceutical, biotechnology and life sciences, consumer research, hospitality, insurance and telecommunications.

Professional Activities

Mr. Ng is a member of the Law Society of Upper Canada, the International Technology Law Association (ITechLaw, formerly the Computer Law Association), the Canadian Information Technology Law Association, the American Bar Association and the ABA Committee on Cyberspace Law.

Publications

Mr. Ng is a contributor to the Canadian law chapter of the CCH publication, *International eCommerce: Business and Legal Issues*. He is the author of the "Privacy" and "E-Commerce" chapters of Stikeman Elliott's *Doing Business in Canada* publication.

Speaking Engagements

Mr. Ng has hosted numerous in-house and external client presentations involving technology, e-commerce transactions, the implementation of privacy practices and ongoing compliance with privacy policies. Recent speaking engagements include:

- > "Fixing a Problem Outsourcing" at the Centre for Outsourcing Research and Education in Toronto.
- > "Privacy Patchwork" at the Private Sector Privacy Conference in Vancouver.
- > "Privacy Compliance" at the Ultimate Corporate Counsel Conference in Toronto.

- > "Best Practices for Ecommerce Transactions" at the Canadian Institute in Toronto.
- > "Key Issues in Technology Acquisitions" at the IT.CAN-LSUC IT Law Spring Training Program.

Education

Osgoode Hall Law School (LL.B. 1998), University of Western Ontario (BA 1995).

Bar Admission

Ontario Bar, 2000.



David Elder

Suite 1600, 50 O'Connor Street, Ottawa, Canada K1P 6L2
Direct: (613) 564-0532 Fax: (613) 230-8877 delder@stikeman.com

Law Practice

David Elder practices communications, competition and privacy law in the Ottawa office, where he is a member of the Communications, Competition, Government Relations, Regulatory and Public Policy practice groups. He is a highly-regarded practitioner with over 20 years experience gained in private practice, government and corporate settings. David was formerly Vice President, Regulatory Law with Bell Canada, where he also served as Bell Privacy Ombudsman, the equivalent of Chief Privacy Officer. He has also served as Legal Counsel to the CRTC.

David has provided legal and strategic advice with respect to a wide range of broadcasting and telecommunications proceedings, including those relating to licensing, policy matters and competitive disputes. In various written, oral, expedited and dispute resolution proceedings he has advocated on behalf of clients before the CRTC, Industry Canada, the Federal Court of Appeal, the Privacy Commissioner of Canada and several Parliamentary Committees and working groups.

He serves a broad range of clients in the communications industry including broadcasters, broadcasting distributors, Internet content providers, software-as-a-service providers, property developers, government departments and agencies, industry associations and telecommunications service providers employing Internet, wired, wireless and satellite technologies.

David has been recognized in The 2011 Chambers Global's *The World's Leading Lawyers for Business* as a recommended lawyer in Telecommunications & Broadcasting.

Professional Activities

David has been an active member of the Information Technology Association of Canada and the Canadian Wireless Telecommunications Association. He is the former chair of the Lawful Access Committee of the Canadian Association of Internet Providers and a former member of the Steering Committee of the 45th Circuit program of the Ottawa Centre for Research and Innovation and the Steering Committee for the biennial Law Society of Upper Canada / Canadian Bar Association Communications Law and Policy Conference.

Community

David has also been a fundraising leader for the Bell Walk for Kids Help Phone, winning the Inspiration Award for the highest fundraising of an Ottawa-based team in both 2007 and 2008. He is also a community volunteer and Board Member of the Sir Ernest MacMillan Memorial Foundation, a charitable organization that provides financial support to young musicians in the pursuit of their advanced education and career development.

Selected Presentations and Publications

- > "Court awards first ever damage award under Canadian private sector privacy legislation", *BNA World Data Protection Report*, January 2011.
- > "Privacy "What if?": no medical files, no compensation", *Privacy Scan*, 26 October, 2010.
- > "Privacy "What if?": the game show approach to surveillance", *Privacy Scan*, 22 October, 2010.
- > "A Year in Privacy: Highlights from the Courts and the Commissioner", *Meeting Your Privacy Obligations*, Canadian Institute, Toronto, 12 May 2010.
- > "The Matter of Local Television: Conventional Broadcasting at the Crossroads," (2010), *New Developments in Communications Law and Policy*, Law Society of Upper Canada/Canadian Bar Association, 23 April 2010. (co-author Sheridan Scott).
- > "Goin' Mobile: The Future of Wireless Competition", *8th Annual Canadian Telecommunications Forum*, Ottawa, 30 November 2009.
- > "Lawful access legislation, the sequel: more tools for law enforcement, more concerns for privacy advocates", *Privacy Scan*, 11 September 2009.
- > "Telecommunications Common Carriers and Subscriber Privacy: 'Collateral Damage' in the War on Terrorism?" (2002), *New Developments in Communications Law and Policy*, Law Society of Upper Canada/Canadian Bar Association.
- > "Changing Communications Regulation in the Information Age," (2000), 14 C.J.A.L.P. 153 (co-author Sheridan Scott).
- > David speaks regularly on communications and privacy matters.

Education

University of Ottawa (LL.B. 1989); York University (B.A. (Hons.) English Lit./Mass Com. 1985).

Background

Immediately prior to joining Stikeman Elliott, David had his own law practice in Ottawa, specializing in communications and privacy law.

Bar Admission

Ontario, 1991.



Karen E. Jackson

5300 Commerce Court West, 199 Bay Street, Toronto, Canada M5L 1B9
Direct: (416) 869-5601 Fax: (416) 947-0866 kjackson@stikeman.com

Law Practice

Karen Jackson is a senior partner in Stikeman Elliott's Corporate Group. She practices primarily in the areas of mergers and acquisitions, joint ventures, privacy and outsourcing. She is the firm's Chief Privacy Officer. A significant part of her work involves cross-border transactions. Ms. Jackson is a member of the firm's Technology and Outsourcing Group (which includes the firm's privacy practice), the M&A/Private Equity Group, the Mining Group and the Energy Group.

Professional Activities

Ms. Jackson is a member of the International Technology Law Association. She is also involved in community activities including as a director of Plan International Canada Inc. and Peggy Baker Dance Projects.

Publications & Speaking Engagements

- > Speaker at the International Joint Venture Course presented by Federated Press in December 2009. Topic: "International Joint Venture Governance."
- > Speaker at the 6th Structuring Venture Capital & Private Equity Transaction Course presented by Federated Press in October 2008. Topic: "Structuring Purchase and Sale Agreements."
- > Speaker at the 2nd Annual Ultimate Corporate Counsel Conference presented by the Canadian Corporate Counsel Association in November 2007. Topic: "Responding to a Privacy Breach under Federal, Alberta and British Columbia Legislation."

Representative Transactions

Lead counsel to:

- > companies in the financial services, retail and other sectors, including US retailers expanding into Canada, in connection with privacy law issues
- > a publicly listed Canadian mining company in its negotiations with an international mining company to establish a joint venture to develop a \$4B iron ore mine
- > LS-Nikko Copper Inc. and Korea Resources Corporation in connection with LS-Nikko's acquisition of an option to acquire a 20% interest in Inmet Mining Corporation's copper project in Panama, which has an estimated capital cost of US \$3.5B
- > Bell Canada Inc. in connection with wireline outsourcing arrangements between Bell Canada and Bell Alliant Regional Communications Inc.
- > a US company in connection with its provision of a trading platform and related services to a subsidiary of a Canadian bank

Co-counsel to:

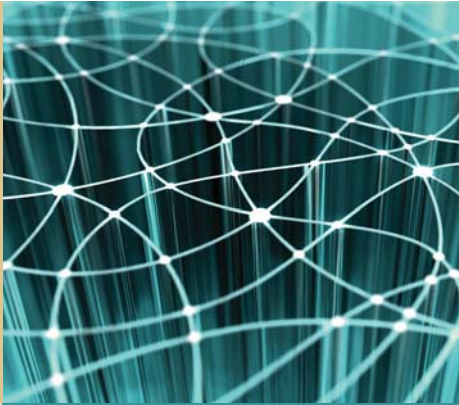
- > a major US retailer in connection with a privacy breach involving the theft of more than 46 million credit and debit card numbers and a joint investigation by the federal and Alberta Privacy Commissioners
- > Sithe Global Power, LLC with respect to establishing its Goreway Station Partnership, the owner of a \$1B electricity generation facility and the subsequent sales of Sithe's partnership interests to Chubu Electric Power Goreway B.V. and Toyota Tsusho Goreway Netherlands B.V.
- > Amulet Limited and Advisors (Canada) ULC in connection with Amulet's subscription for \$100M of senior secured notes of Yamana Gold Inc., the proceeds of which are being used to develop a gold mine in Brazil

Education

York University (MBA 1982), Osgoode Hall (LL.B. 1977), University of Toronto (B.Sc. 1974).

Bar Admission

Ontario, 1979.



SEMINAR WEDNESDAY, APRIL 13, 2011

SPAM AND PRIVACY UPDATE

Are you compliant?

PRESENTATION SLIDES

The Wide Net of Canada's New Anti-Spam Legislation
David Elder

Canadian Privacy Law: Online Tracking and Recent Developments
Karen Jackson



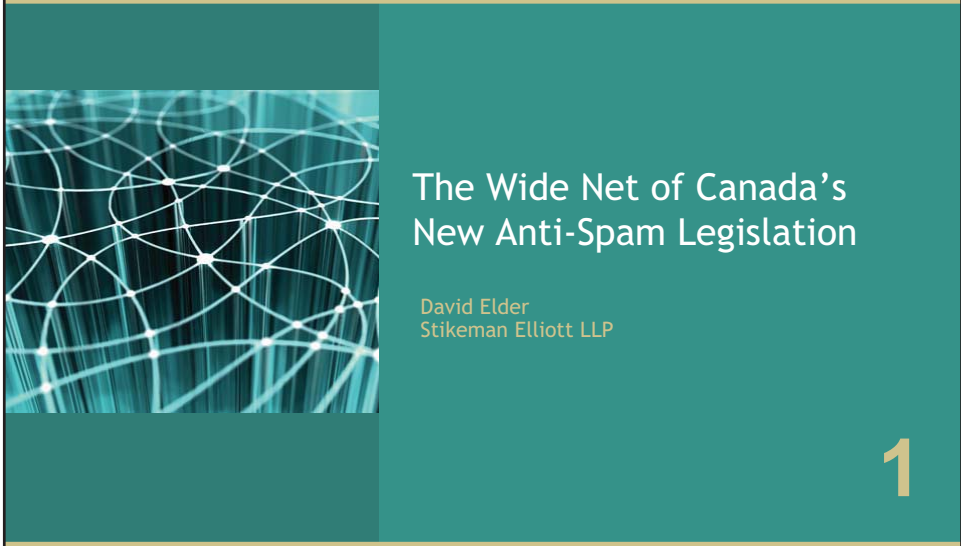
Topic Overview

1. The Wide Net of Canada's New Anti-Spam Legislation
- *David Elder*
2. Canadian Privacy Law: Online Tracking and Recent Developments
- *Karen Jackson*

SLIDE 1

STIKEMAN ELLIOTT LLP

STIKEMAN ELLIOTT



The Wide Net of Canada's New Anti-Spam Legislation

David Elder
Stikeman Elliott LLP

1

STIKEMAN ELLIOTT LLP www.stikeman.com



Bill C-28: The Unnamed Anti-Spam Legislation

- History and status
- Amends *CRTC Act*, *Competition Act*, *PIPEDA*, *Telecommunications Act*
- CRTC as main overseer...at least for now, but Commissioner of Competition and Privacy Commissioner also have roles
- Largely supplants control over spam through privacy law
- Intended to deter “most damaging and deceptive” spam and related threats: identity theft, phishing, pharming spyware, viruses, botnets
- Will broad brush approach sweep in more legitimate activity?

SLIDE 3

STIKEMAN ELLIOTT LLP



What it does

- Prohibits sending commercial electronic messages without express consent (some exceptions)
- Creates identification, contact and unsubscribe obligations
- Prohibits the installation of a computer program without express consent (some exceptions)
- Prohibits the alteration of transmission data or rerouting of messages without express consent
- Creates detailed disclosure requirements to obtain consent
- Creates significant monetary penalties for non-compliance
- Creates private right of action for damages stemming from contraventions

SLIDE 4

STIKEMAN ELLIOTT LLP




What it also does

- Amends the *Competition Act* to prohibit false or misleading commercial representations that are made electronically
- Amends *PIPEDA* to prohibit collection of personal information through address harvesting, unauthorized access to computer system
- Sets the stage for amendments to the *Telecommunications Act* for future reform of current DNCL/telemarketing regime - could result in opt-in approach

SLIDE 5

STIKEMAN ELLIOTT LLP



Scope - Key Definitions

“electronic message” means a message sent by any means of telecommunication, including a text, sound, voice or image message.

“commercial activity” means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada.

SLIDE 6

STIKEMAN ELLIOTT LLP

Commercial Electronic Message

- An electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including an electronic message that:
 - a) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
 - b) offers to provide a business, investment or gaming opportunity;
 - c) advertises or promotes anything referred to in paragraph (a) or (b); or
 - d) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs a) to (c), or who intends to do so.

SLIDE 7

STIKEMAN ELLIOTT LLP

Core Anti-Spam Provision

- prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless:
 1. Have the express or implied consent of the recipient
 2. Message is in the prescribed form:
 - identifies sender/person on whose behalf sent
 - contact info for sender/person on whose behalf sent
 3. No cost, easy unsubscribe mechanism:
 - Same means as message sent, or other electronic means
 - Gives Electronic address/web link for unsubscribe
 - Effective “without delay”, no later than 10 business days

SLIDE 8

STIKEMAN ELLIOTT LLP

Exemptions

From Consent and Form

- recipient engaged in commercial activity, message consists solely of a related inquiry/application
- Interactive voice calls, facsimile calls to telephone account or voice recordings sent to telephone account
- as provided in regulations
- TSP - mere conduit

From Consent only

- Requested quote or estimate
- Completes/confirms transaction
- Warranty, recall, safety
- factual info - subscription
- Info re employment
- Good or service entitled to receive

SLIDE 9

STIKEMAN ELLIOTT LLP

Implied consent

- Existing business relationship:
 - Purchase, sale or barter of goods or services within previous 2 years
 - Acceptance of business opportunity within previous 2 years
 - Written contract, in force, or expired within previous 2 years
- Conspicuous publication of electronic address
- Disclosure by recipient of “business card” info
 - ...without caveat, where message relevant to function/role/duties
- Transitional “Grandfathered” existing business relationship

SLIDE 10

STIKEMAN ELLIOTT LLP



Altering transmission data

- Prohibited, in course of commercial activity, to alter/cause to be altered transmission data of electronic message to deliver to alternate address unless:
 - Express consent of sender/person on whose behalf sent
 - Must provide ongoing “unconsent” electronic address
 - Implement “without delay” and within 10 business days
 - Made pursuant to court order

SLIDE 11

STIKEMAN ELLIOTT LLP



Installation of Computer Program

- Must not install/cause to be installed a “computer program” on other’s “computer system”
- Must not cause electronic message to be sent
- Unless:
 - Express consent of owner/authorized user
 - Provide electronic address for remove/disable - for 1 year
 - Provide no-cost assistance re remove/disable request
 - Acting pursuant to court order

SLIDE 12

STIKEMAN ELLIOTT LLP

Express Consent

- Must set out “clearly and simply”:
 - Purpose or purposes for which consent sought
 - Prescribed info identifying sender/person on whose behalf sent
 - Other prescribed info
 - For computer programs, clear general description of function and purpose
 - Enhanced requirements for certain program functions contrary to reasonable expectation of user
- Also transitional “grandfathered” consent

SLIDE 13

STIKEMAN ELLIOTT LLP

“Unreasonable” functions

- Collection of personal info stored on computer
- Interfering with owner/user control of computer
- Changing/interfering with settings, preferences or commands - without knowledge of owner/user
- Changing/interfering with data stored on computer so as to interfere with “lawful access” to or use of data
- Unauthorized communication with other computer, device
- Capability of unknown/unauthorized 3rd party activation

SLIDE 14

STIKEMAN ELLIOTT LLP

Express Consent - Programs

- Express consent for installation if program is
 - A cookie
 - html code
 - Java script
 - Operating system
 - Executable only through use of another program installed with consent
 - As per Regs
- AND conduct suggests reasonable to believe they consented (?)

SLIDE 15

STIKEMAN ELLIOTT LLP

The “Teeth”

Investigation

- Preservation demand
- Notice to produce
- Search warrant

Enforcement

- AMPs for “violations”
 - Up to \$ 1 M individual, \$ 10 M corporate
- Undertakings
- Public shaming
- Registration with court - enforced as contempt
- Injunctions, Restraining Orders
- Offences
- Private right of action

SLIDE 16

STIKEMAN ELLIOTT LLP



Client To Do List

- Review/modify practices for obtaining eMarketing lists, choose vendors/partners carefully
- Review/modify formats for eMarketing
- Ensure effective and timely unsubscribe
- Review/modify program installations, associated disclosures and consent
- Ensure consent records are retained and retrievable
- Engagement of marketing, brand, technical resources to detect issues, ensure compliance

SLIDE 17

STIKEMAN ELLIOTT LLP

STIKEMAN ELLIOTT



Canadian Privacy Law: Online Tracking and Recent Developments

Karen Jackson
Stikeman Elliott LLP

2

STIKEMAN ELLIOTT LLP www.stikeman.com

Canadian Privacy Law

- Online Tracking
 - Digital Markers
 - Deep Packet Inspection
 - Personal Information
 - Consent
 - Use
- Recent Developments
 - Amendments
 - Decisions of Commissioners
 - Court Decisions

SLIDE 19

STIKEMAN ELLIOTT LLP

ONLINE TRACKING

Digital Markers

- Digital markers collect information from Internet users as they browse websites
- Three common types of markers - HTTP or HTML cookies, Flash cookies and web beacons
- Digital markers produce log files that contain information about usage patterns and browsing history
 - IP addresses, user preferences
 - pages visited, length of time spent on pages
 - search queries entered
 - geographical location
- This information can be connected to user identities through user names and credit card numbers entered by individuals on web pages or when IP addresses can be attributed to an individual

SLIDE 20

STIKEMAN ELLIOTT LLP

ONLINE TRACKING



Deep Packet Inspection

- DPI gives third parties the ability to view and inspect “digital packets” of information transmitted from one Internet user to another via email, VOIP, peer-to-peer file sharing, etc.
- DPI can also be used to help an ISP manage network traffic
- Content is not always inspected - an ISP may inspect the application layer of a “packet” which only allows it to see the type of software application being used

SLIDE 21

STIKEMAN ELLIOTT LLP

ONLINE TRACKING



Behavioral Advertising

- Behavioral advertising uses the information gathered from digital markers and DPI to construct user profiles and display online advertisements optimized to user interests
- Many individuals view personalization of advertisements positively - however personalization necessitates some loss of privacy

SLIDE 22

STIKEMAN ELLIOTT LLP

ONLINE TRACKING

Personal Information

- In the 2003 Air Carrier case, the federal Commissioner determined that information stored on both temporary and permanent cookies was personal information
- In the 2009 Bell Sympatico/DPI case, the Assistant Commissioner held that IP addresses may be personal information if they can be linked to an identifiable individual
- Significant uncertainty remains as to when information collected online is transformed from data to personal information

SLIDE 23

STIKEMAN ELLIOTT LLP

ONLINE TRACKING

Consent

- Individuals must understand what personal information is being collected online and how it will be used
- Implied consent - organizations should consider the sensitivity of the information and whether the manner of collection is reasonable
- Opt-in consent - favored by the OPC
 - as of May 25, 2011 the European Union will require websites to obtain express consent from users before cookies can be used
- Opt-out consent - OPC has stated that organizations should use opt-out consent for online tracking only if:
 - the personal information collected is not sensitive
 - the type of information disclosed for marketing purposes and the extent of the intended use or disclosure should be well defined and clear to the individual at the time he or she has the opportunity to opt-out

SLIDE 24

STIKEMAN ELLIOTT LLP

ONLINE TRACKING

Use

- Personal information can only be used for purposes a reasonable person would consider appropriate in the circumstances
 - specific personal information utilized
 - the advertiser
 - the specific ad
- Individuals receive many valuable and convenient services online for free, so they should realize advertising revenues need to be generated to support websites

SLIDE 25

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: AMENDMENTS

PIPEDA - Bill C-28, The Anti-Spam Act

- Privacy Commissioner can now decide not to investigate a complaint if:
 - complainant has not exhausted other grievance/review procedures
 - complaint could be more appropriately dealt with under another law
 - complaint not filed within a reasonable time
- Privacy Commissioner can stop an investigation if:
 - any of the reasons listed above become applicable
 - there is insufficient evidence to pursue the complaint
 - the complaint is trivial, frivolous or vexatious or made in bad faith
 - the organization has provided a fair and reasonable response
 - the subject matter has already been dealt with by the Commissioner
 - the matter is being or has been addressed in another grievance or review process or under another law

SLIDE 26

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: AMENDMENTS

Bill C-29, Safeguarding Canadians' Personal Information Act

- Died with the dissolution of Parliament on March 26, 2011
- It would have created a business transaction exception for the use and disclosure of personal information
- Also, would have required notification to the Commissioner of material privacy breaches and notification to individuals if the privacy breach created a real risk of significant harm

SLIDE 27

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: AMENDMENTS

AB PIPA: Breach Notification

- PIPA was amended effective May 1, 2010 to include breach notification requirements and notification policies and practices relating to foreign service providers
- Breach notification requirements:
 - Commissioner must be notified of privacy breaches if there is “a real risk of significant harm”
 - Commissioner can then decide to direct the organization to notify affected individual(s) of the breach
 - notification must be given directly to affected individual(s) unless Commissioner determines that direct notification would be unreasonable in the circumstances

SLIDE 28

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: AMENDMENTS

AB PIPA: Foreign Service Providers

- An organization that has a foreign service provider collect or use personal information must notify affected individuals about:
 - how they can obtain information regarding the organization's policies and practices with respect to the foreign service provider
 - the purposes of the collection of their personal information
 - contact information for someone who can answer questions
 - the personal information that is collected by, or transferred to, the service provider
- An organization's personal information policies and practices must include:
 - information regarding the countries, other than Canada, in which personal information is collected, used, disclosed or stored
 - the purposes for which the service provider has been authorized to collect, use or disclose personal information

SLIDE 29

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: DECISIONS OF COMMISSIONERS

PIPEDA Case Summary #2009-021

- A debt collection agency found that the complainant was the co-owner of a home when it searched land registry records in connection with debt collection activities relating to another individual's VISA account
- It disclosed this information to the bank that was owed the VISA debt and to the Ontario government when responding to a complaint about the agencies debt collection activities
- Assistant Commissioner determined that the personal information was publicly available and could be collected, used and disclosed without consent
 - the decision did not discuss "relate directly to the purpose for which the information appears in the registry"

SLIDE 30

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: DECISIONS OF COMMISSIONERS



PIPEDA Case Summary #2010-003

- This case was about an access request that was mishandled by a major telecommunications company
- The moral of the story: organizations should look at their regular deletion/retention practices when they receive an access request to determine if they need to be overridden

SLIDE 31

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: DECISIONS OF COMMISSIONERS



Google Street View Case

- The Commissioner found that Google collected emails, phone numbers, credit card numbers, SINS and other personal information without consent
- The personal information was collected as a result of a code integrated into the software used by Google Street View
- The engineer responsible for the code had identified “superficial privacy implications” but those implications were not assessed because the engineer did not forward his design documents to Google’s lawyers, contrary to Google’s policies
- This case emphasizes the importance of consistently applying internal privacy policies (i.e. by training staff or by appointing individuals to be accountable for compliance with the policies) so as to avert easily preventable violations of privacy laws

SLIDE 32

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: DECISIONS OF COMMISSIONERS



BC PIPA Order P10-01

- Restaurant had a policy of requiring all customers to present ID prior to serving them alcohol
- 60-year-old customer complained and the adjudicator determined the restaurant should collect identification about customers only if there is a reasonable basis to suspect that they may not be of legal drinking age

SLIDE 33

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS



Stevens v. SNF Maritime Metals Inc. (2010 FC 1137)

- Stevens was employed at a company which supplied scrap metal to SNF Maritime Metals Inc.
- Stevens opened his own account at SNF and had scrap metal he delivered to SNF credited to his personal account
- SNF provided the employer with Stevens' personal account statements and the employer subsequently fired Stevens
- Federal Court refused to award damages to Stevens because it found the damages Stevens claimed were all tied to the termination of his employment, not the breach of PIPEDA

SLIDE 34

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS



Randall v. Nubodys Fitness Centres (2010 FC 681)

- Randall's employer sponsored his membership at Nubodys and Nubodys regularly informed the employer about the number of times Randall went to Nubodys
- Federal Court did not award damages for the breach of privacy
- It held an award of damages under PIPEDA was not to be made lightly, damages are awarded where the breach of a very serious and violating nature such as video-taping and phone-line tapping
- It also stated that the breach was not the result of malicious behaviour which would justify an award of damages

SLIDE 35

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS



Compagnie d'assurances Standard Life c. Tremblay, (2010 QCCA 933)

- Tremblay was receiving disability benefits from Standard Life
- Standard Life's medical consultant suggested surveillance and Standard Life monitored Tremblay on 5 different occasions
- During the 2nd surveillance session, the investigators accidentally recorded Tremblay's brother engaging in very active tasks and Standard Life terminated Tremblay's benefits

SLIDE 36

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

Compagnie d'assurances Standard Life c. Tremblay, (2010 QCCA 933) (cont'd)

- Quebec C of A upheld the trial judge's decision that Standard Life did not have a good reason to order the surveillance and consequently, committed a significant violation of Tremblay's privacy
 - insurer can undertake surveillance if it is necessary to discover the truth
 - there must be serious reasons to doubt the honesty of the individual
 - the test is proportionality
- It also deferred to the trial judge's assertion that Tremblay's dignity was ruined and his reputation damaged and upheld a punitive damage award of \$100,000

SLIDE 37

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

Nammo v. Transunion of Canada Inc. (2010 FC 1284)

- Transunion's credit profile of Nammo included the credit history of another individual
- Nammo was denied a bank loan as a result of this incorrect credit profile
- Federal Court held that Transunion breached PIPEDA's accuracy principle
- Nammo received damages of \$5,000 for humiliation even though there was little evidence relating to humiliation

SLIDE 38

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada (2010 FC 736)

- Federal Court determined that the collection of evidence by an insurer acting for an insured in the defence of a third party tort action was not “commercial activity” within PIPEDA
- If the primary activity is the collection of evidence by an individual defendant and that activity is not commercial activity, the activity retains its non-commercial nature even if third parties are retained by the individual to carry out the activity

SLIDE 39

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

Mosher v. Coast Publishing Ltd. (2010 NSSC 153) & *Warman v. Wilkins-Fournier*, (2010 ONSC 2126)

- These decisions show the conflicting approaches courts have used to determine whether an organization can be compelled to reveal the identity of an online commentator who allegedly posted defamatory comments
- Nova Scotia SC ordered disclosure, stating “The court does not condone the conduct of anonymous internet users who make defamatory comments and they like other people have to be accountable for their actions.”
- Ontario SC did not order disclosure because a prima facie case of defamation had not been established
- It said “The requirement to demonstrate a prima facie case of defamation furthers the objective of balancing the public interest in favour of disclosure and the legitimate interests of privacy and freedom of expression.”

SLIDE 40

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

Privacy Commissioner of Canada v. Air Canada (2010 FC 429)

- This case is related to the SCC's decision in the Blood Tribe case which held that the Privacy Commissioner cannot rule on an assertion of privilege and cannot inspect documents over which privilege is claimed
- In this case, the Commissioner claimed that under section 12 she is entitled to require Air Canada to justify its assertion of privilege by way of a detailed affidavit
- Federal Court held that since the Commissioner cannot make decisions with respect to claims of solicitor-client privilege, the Commissioner cannot require a party to justify its claim for privilege

SLIDE 41

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

Larose c. Banque Nationale du Canada (2010 QCCS 5385)

- This is the first class action arising from a privacy breach to be certified in Quebec

Citi Cards Canada v. Pleasance (2011 ONCA 3)

- This case relates to a request by Citi Cards to TD for mortgage or discharge statements
- It suggests that exemptions under PIPEDA for disclosure without consent will be read narrowly in order to protect the privacy of an affected individual
- Institutions providing mortgage statements to third parties, without consent and in the absence of a judicial order, are breaching their clients' privacy rights

SLIDE 42

STIKEMAN ELLIOTT LLP

RECENT DEVELOPMENTS: COURT DECISIONS

R. v. Cole (2011 ONCA 218)

- A high school teacher was provided with a laptop by the school
- School had a policy which permitted personal use of such laptops but expressly prohibited use or storage of inappropriate content
- Ontario C of A concluded that the teacher had a reasonable expectation of privacy in the personal use of the laptop but that he had no expectation of privacy with respect to access by the school's technician for purpose of maintaining the integrity of the school's network
- Important for employers to have clear and explicit policies relating to the personal use of laptops and other equipment which set out the extent to which the employer will be monitoring the employees use of such equipment

SLIDE 43

STIKEMAN ELLIOTT LLP

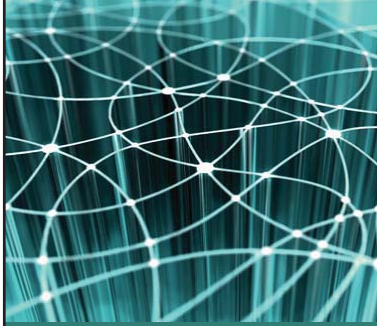
RECENT DEVELOPMENTS: COURT DECISIONS

Jones v. Tsige (2011 ONSC 1475)

- Jones claimed Tsige, her co-worker at a bank, had committed the tort of invasion of privacy by accessing Jones' private banking records
- Ontario SC held there was no common law tort of invasion of privacy
 - C of A decision in *Euteneier*
 - statutory schemes exist to govern privacy issues and remedies available

SLIDE 44

STIKEMAN ELLIOTT LLP



For further information

David Elder
delder@stikeman.com

Karen Jackson
kjackson@stikeman.com

SPAM AND PRIVACY UPDATE

Are you compliant?

ARTICLES

"Spam's big Hammer"

Andi Balla, *CanadianLawyermag.com*

"Time to take steps assuring compliance of new spam law"

Drew Hasselback, *Financial Post*

"Canadian anti-spam legislation on fast-track"

David Elder

"Anti-spam law governs software – not just email"

David Elder, *The Lawyers Weekly*

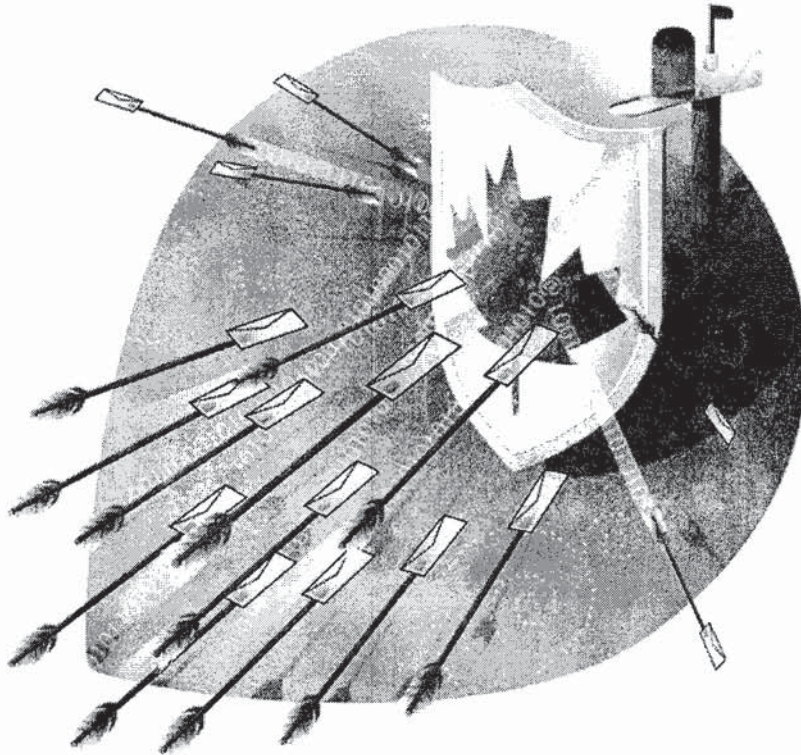
[Additional Links](#)

SEMINAR WEDNESDAY, APRIL 13, 2011

Spam's big hammer

Aiming to fight rogue operators, anti-spam regulations open the door for fines and private action even against legitimate businesses.

BY ANDI BALLA



By the time the Canadian government decided it needed to get tougher on unsolicited marketing via electronic messages in 2008, the country had earned the dubious distinction of being the world's fourth-largest originator of spam. Canada was also the only G8 country to have no anti-spam legislation. Add to the mix an Internet infrastructure that makes it one of the most wired countries in the world, and Canada had the potential to be the perfect breeding ground for more spammers.

That potential did not go unnoticed in Ottawa, which vowed to act to "drive the spammers out," introducing Bill C-28 that is now one of the strictest anti-spam and

electronic protection laws in the world. It received Royal assent on Dec. 15. The bill survived a prorogation of Parliament and tough political discussions — so much so there wasn't even agreement on an official name for the act — the "fighting internet and wireless spam act" is just what everyone calls it colloquially. Now law, Bill C-28 mandates electronic marketing messages cannot deceive the receiver in any way. It also makes receiving messages an opt-in affair, which means permission will be needed to send an e-mail, though there are some important exceptions. Coming into full force in September, the law empowers the Canadian Radio-television and Telecommunications Commission to issue fines of up to \$10 million for companies and \$1 million for individuals. The

act also opens the door for private action, which could lead to damages in court per message sent. If it becomes a class action, the numbers would grow proportionally.

But while the government says Bill C-28 is intended to fight the worst spammers, the anti-spam regulations clearly open the door for high penalties against legitimate businesses, causing concern for some. It is a particularly big change for Canadian companies that engage in electronic marketing, says David Elder, a privacy lawyer with Stikeman Elliott LLP. "The anti-spam legislation essentially prohibits commercial electronic messages without consent, and in most cases, the consent that would be required would be an explicit consent," he says. "So it is very broadly cast. This legislation says it is an opt-in, so companies will need to make sure that it is either within one of the exceptions, or they do have the recipient's consent. That's going to be a big change."

The important exceptions include existing business relationships, which under the law means if a company has done business with an individual in the past two years, then consent is implied. But obviously compliance with the law means companies are now going to have to keep track of when they last did business with the receiver and continually update that list, adds Elder. These new compliance measures and the potentially hefty penalties that come with the new law worry businesses that now face a new playing field. "We are spending an increasing amount of time navigating the compliance issues with the act, given that the potential penalties for non-compliance are so significant," says Adam Kardash, a partner with Heenan Blaikie LLP.

Kardash says while there are exceptions for implied consent, the risk is high enough that many organizations will need

PHANTOM

to thoroughly review their practices. "The existing business-relationship exception will allow many organizations to continue their electronic marketing communications, but they will have to do so . . . following specific rules related to an unsubscribe process, and they will have to carefully manage the time periods for the definition of a business relationship," says Kardash.

The wide implications were not lost on Parliament as it discussed the bill tabled by the Conservative government. Both the NDP and Liberals asked for further clarifications due to cost concerns and making sure large, obvious offenders are targeted instead of legitimate businesses. "There are all kinds of booby traps in this legislation," NDP MP Charlie Angus told Parliament as it discussed the law. "Legislation always has unintended consequences. If we do not do the due diligence, we end up using a hammer to whack a bunch of little pieces all over the place without necessarily getting what we wanted."

Federal Industry Minister Tony Clement says the legislation is meant to deter the most damaging and deceptive spam and other online threats and create a safer online marketplace for both individuals and businesses. "Our government took action through this legislation to reduce a considerable threat to electronic commerce in this country," says Clement.

While the obvious large offenders Angus and Clement are talking about are the ones filling inboxes with offers for cures for erectile dysfunction and fake Rolex watches, the type of shady messages that make up the vast majority of spam (at one point last year, nine out of every 10 messages clogging up some e-mail networks were spam), Bill C-28 will have a major effect on legitimate businesses that send large amounts of communications. "I think that once companies start to examine their marketing practices and their e-mailing practices, they will start to discover that they are going to have

to change some things in all likelihood looking forward — even if they don't consider themselves to be spammers," says Elder.

Law firms, for example, will routinely send out communications to a client list, but under the new legislation they will have to verify they are only sending these to clients active in the past two years or people who asked for the bulletins. "People need to take a step back and come up with an inventory of communications that they are allowed to send out," adds Elder.

But what makes the Canadian law interesting, perhaps because it comes seven years after its American counterpart — an eternity in the Internet age — is how much stricter and all encompassing it is than the U.S. CAN-SPAM Act. "This piece of legislation is above and beyond what we saw in the U.S.," says Roland Hung, a lawyer with Gowling Lafleur Henderson LLP in Calgary. "If this is not one of the most stringent



ELECTRONIC DOCUMENTS RECORDS MANAGEMENT, E-DISCOVERY AND TRIAL

*Editors: Bryan Finlay Q.C., Marie-Andrée Vermette and Michael Statham
With contributions from: Caroline Abela, Stephen Daak, Paul D. Guy, Nikiforos Iatrou,
Stephanie L. Turnham, David Vitale and John Wilkinson*

EFFECTIVELY NAVIGATE THE LEGAL CHALLENGES POSED BY ELECTRONIC DOCUMENTS

Electronic data is modifying how lawyers interact, changing how information is collected and used, and transforming the courtrooms.

This in-depth resource examines and analyzes the issues relating to electronic documents, including:

- the sources and types of electronic documents
- records management policies
- the legal framework governing e-discovery in Canada
- the preservation, collection, processing, review and production of electronic documents
- the use of electronic evidence at trial

Visit canadalawbook.ca or call 1.800.565.6967 for a 30-day no-risk evaluation

Looseleaf • \$210
Subscription updates
Invoiced as issued (1/yr)
P/C 0283030000
ISSN 1920-1737

Prices subject to change without notice,
to applicable taxes and shipping & handling.

CANADA LAW BOOK



THOMSON REUTERS

CL0311

legislations around in the world, I would have to say we are up to par.”

For one, the U.S. law deals only with e-mail spam, while in Canada the legislation covers all electronic messages, phishing, and spyware. “In the U.S. all they need to do is have an opt-out option, where as in Canada, we are way more strict, and under the new law you’d actually have to obtain consent even before sending,” says Hung. “The law is drafted in such a way that makes it very broad, and it factors any type of commercial electronic messages.”

Another important factor of the legislation is that beyond a regulator’s actions, it specifically gives spam victims the power to take private right of action and that could potentially lead to class actions if a lot of people decide to act in unison towards perceived spam. “There is clearly litigation risk associated with the legislation,” says Kardash. “For prudent organizations there is a due diligence defence, but there will be litigation involving rogue actors, like major spammers, which is precisely the key target of this legislation in the first place.”

While the anti-spam legislation is now law, there are also a series of amendments to Canada’s mammoth privacy legislation, the Personal Information Protection and Electronic Documents Act, that are currently in the pipeline and relate to this issue. Some of the PIPEDA changes are dictated by Bill C-28, others are not. The bill clearly states that it amends PIPEDA, says Hung. “One of the vital changes to PIPEDA is that if there is a computer program going around, collecting personal information, this is no longer allowed. It changes PIPEDA to explicitly prohibit this.” That relates to computer programs that randomly harvest e-mail addresses from the Internet to later send them unsolicited messages.

Only time will tell what will happen once the changes become mandatory in September. But the government says, based on the experience of other countries with similar legislation, it expects noticeable results quickly. The year after Australia passed similar legislation in 2004, for example, it dropped out of the world’s top 10 spam-originating countries. “The intent of the proposed law is to deter the most damaging and deceptive forms of spam from occurring in Canada and help drive spammers out of Canada,” the government noted in its policy statement of the new act, adding several of Canada’s global partners, such as Australia, the United Kingdom, and the U.S., have passed strong domestic laws to combat spam and related online threats.

It’s also important to note the new legislation doesn’t apply to non-commercial activity. Political parties and charities that engage Canadians through e-mail are not subject to it if these communications do not involve selling or promoting a product.

The problem is there is some uncertainty of how far the government regulators will take the implementation of the law. For example, there is a whole host of list-brokerage activity that would be considered in the marketing community as entirely legitimate, yet the current form of the act may result in certain e-mail list-brokerage activity being significantly curtailed.

And with marketing evolving with the web, it is not fully clear what the law will and will not cover. “For example, in electronic space, there are viral marketing-related tools for campaigns such as invite-a-friend or send-a-friend, and it will be important to ensure that these are not unintentionally caught by the statutory framework as they have become a critical tool for marketing in the digital space,” says Kardash. ■

Time to take steps assuring compliance of new spam law

Drew Hasselback, Financial Post · Jan. 5, 2011



Change is afoot for those who rely on email for marketing.

The federal government has passed a law that will bar the sending of unsolicited email or spam.

Bill C-28, the Fighting Internet and Wireless Spam bill, was granted Royal Assent in December and should be in force by summer, lawyers say. This gives corporate counsel several months to begin talks with IT departments to ensure their companies are in compliance.

The legislation is supposed to apply to any electronic message sent over any means of telecommunication, and this should be broad enough to include not just conventional email, but also things such as postings on Twitter or Facebook.

Indeed, Rebecca Chan, partner with Borden Ladner Gervais LLP in Toronto, says corporate counsel should be raising the matter with any staff who deal with social media. "The way it's drafted is technology neutral. So it can pick up other forms of mass communication."

The main thing companies need to ensure is that they are only sending emails to Canadians with their consent. Explicit consent is the easiest approach. When companies collect consumer data, they should make sure they're being forthright about asking consumers whether they want to receive emails in the future. Any messages sent from then on need to contain information on how the consumer can unsubscribe from the list.

The act does allow for implicit consent in narrow circumstances. These include situations where the customer has an existing business relationship with the company, or where recipients freely publish their email addresses on the Web without a statement warning that unsolicited messages are unwelcome.

The act also includes some specific exemptions. For example, companies are allowed to send out unsolicited emails with information about product upgrades or warranties.

Another key provision companies should be aware of is a bar on the installation of programs on consumers' computers without their consent. This is designed to limit the spread of spyware or malware.

Businesses need to ensure that any third-party contractors they hire for marketing campaigns are also in compliance with the new rules. You can't outsource your marketing, then plead ignorance if your contract provider runs afoul of the law.

The act makes it an offence to send false or misleading electronic messages. This refers not just to the content of the message, but also any attempt to mask the sender's identity or location. These provisions are designed to attach to emails that pitch scams. This should only concern reputable companies if their business plans involve connecting heirs with the oil fortunes accumulated by their recently deceased Nigerian uncles.

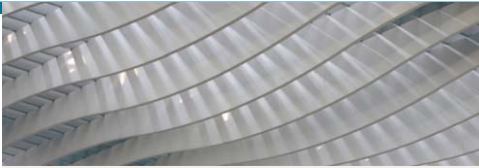
The CRTC is responsible for enforcing the act. Penalties can reach up to \$1-million for individuals and \$10-million for organizations.

An obvious question is whether the law will succeed in reducing or eliminating the amount of unwanted email flowing into your inbox. Unfortunately, the law will have to operate for a few years before anyone can answer that one effectively.

"It raises expectations, but like the Do Not Call List, one wonders," says David Elder, a counsel with Stikeman Elliott LLP in Ottawa. "Certainly the more reputable companies are always going to try to respect the law."

The National Do Not Call List managed by the CRTC is supposed to protect Canadians from receiving unwanted telemarketing calls. Critics, such as University of Ottawa professor Michael Geist, have called it a disaster.

dhasselback@nationalpost.com



David Elder practices

Communications, Competition and Privacy Law in the Ottawa office, where he is a member of the Telecommunications and Broadcasting, Competition, Government Relations, Regulatory and Public Policy practice groups. He is a highly-regarded practitioner with over 20 years experience gained in private practice, government and corporate settings.

Stikeman Elliott's Communications Group consists of partners and associates drawn from the firm's domestic and international law offices possessing expertise in telecommunications and broadcasting law and complementary legal disciplines, including competition, corporate and commercial, and copyright.

The Group is able to draw upon the particular strengths of each of its members in responding to clients' needs. This ensures that our clients receive legal services tailored to their specific needs in a timely and cost-effective manner, regardless of the complexity of the issues or the size of the particular transaction.

The Group has established a blog on legal, legislative and policy developments that can be accessed online at www.CanadianCommunicationsLaw.com

Canadian anti-spam legislation on fast-track

November 2010

David B. Elder (delder@stikeman.com)

The Canadian government's anti-spam bill is moving quickly through Parliament, with only its name apparently lacking support from the opposition parties.

On May 25, 2010, the Canadian government introduced Bill C-28, an act that would establish the federal *Fighting Internet and Wireless Spam Act* and make significant consequential amendments to other federal legislation, including Canada's *Competition Act*, *Telecommunications Act*; and *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Bill C-28 is extremely similar in substance to Bill C-27, which was introduced in April 2009 and titled the *Electronic Commerce Protection Act*. Bill C-27 received unanimous support in the House of Commons following its third reading, but it died upon prorogation in December of 2009 while at the Standing Senate Committee on Transport and Communications. Given the strong resemblance between the two bills, and the fact that the earlier bill had received full consideration by the House Standing Committee on Industry, Science and Technology, the newer bill, Bill C-28 cleared the Committee process after a single meeting. The bill was reported back to the house without amendment – with the exception of the short title, which was opposed by opposition Committee members as being overly dramatic, and not in keeping with naming conventions for Canadian legislation.

Like its predecessor, Bill C-28 was designed to reduce unsolicited or junk e-mail, commonly referred to as “spam”. Most importantly, the legislation aims to bolster consumer confidence in electronic commerce, which the government has described as necessary in order to position Canada as a leader in the digital economy. The bill incorporates a number of the legislative recommendations made in 2005 by the government-mandated “Task Force on Spam”. The proposed legislation aims to regulate activities such as spam, counterfeit websites (known as “phishing”) and spyware.

Bill C-28 would also establish a regime whereby the Canadian Radio-television and Telecommunications Commission (“CRTC”), the Competition Bureau of Canada and the Office of the Privacy Commissioner could share information and evidence with law

enforcement agencies outside Canada, in an effort to enforce similar international laws and pursue violators beyond Canadian borders. Currently Canada is the only G8 country and one of only four OECD (Organisation for Economic Cooperation and Development) countries without specific spam legislation. Thus, when the government first introduced Bill C-27 it was cast as a necessary step in fulfilling Canada's international duty to join global partners in passing laws to combat spam and related cyber threats.

Prohibitions

The anti-spam provisions remain largely unchanged from Bill C-27. They would prohibit sending (or causing or permitting to be sent) a commercial "electronic message" (which is defined broadly to include a text, sound, voice or image message) to an electronic address, unless the recipient has given express or implied consent. Implied consent would apply to situations in which there is an existing business or non-business relationship between the sender and recipient, and to certain limited circumstances where the recipient has, within a business context, conspicuously published or disclosed the electronic address and the disclosure was not accompanied by any statement that the person did not wish to receive commercial messages (there is also a provision that would permit future regulations to further define implied consent).

BILL C-28 also sets requirements for the form of permitted messages: the message must identify the person who sent the message (and, if it is different, the identity of the person on whose behalf the message was sent), along with contact information for those identified. Moreover, permitted messages must include an unsubscribe mechanism, which includes either a hyperlink (valid for at least 60 days after the message is sent) that the recipient can follow, or a specified electronic address to which an unsubscribe request can be sent. Requests must be given effect within 10 days.

The anti-phishing provisions are drafted as prohibitions against "altering transmissions data", and would prohibit the unauthorized redirection of an electronic message to a destination other than or in addition to that specified by the sender, except with the sender's express consent. As with the anti-spam provisions, an electronic address must be provided to which the sender may give a notice of withdrawal of consent, and the request must be given effect within ten days.

Significantly, the new bill also contains provisions, aimed at combating spyware and malware, that would prohibit the installation of computer programs without consent. The bill also sets out requirements that an organization seeking such consent must clearly describe the function and purpose of every program to be installed, going further to disclose "foreseeable impacts" where the function and purpose include one or more of a number of prescribed functions, such as the collection of personal information stored on the computer system. Certain types of code and programs are exempted from these requirements, including html code and javascripts, yet the provision will still have wide-reaching impact on a broad range of legitimate businesses who offer services through downloadable software applications and components.

Notably, the prohibitions in Bill C-28 are broader than those previously provided for in Bill C-27. The prohibitions in both bills apply to anyone who procures or causes to procure a prohibited act. However, the language in Bill C-28 has been extended to also apply where someone aids in or induces such an act.

Administrative Monetary Penalties

Provisions of BILL C-28 that would subject violators of the Act to an Administrative Monetary Penalty ("an AMP") remain the same as those originally envisaged in Bill C-27. An individual who violates any of the foregoing prohibitions may be subject to an AMP of up to \$1 million and corporate entities would be liable to an AMP of up to \$10 million. Officers, directors, and agents of corporations that violate the prohibitions could also be held liable for such actions if they directed, authorized, acquiesced in or participated in the commission of the violation.

Anyone charged under the Act can raise a due diligence defence. They must show that they exercised due diligence to prevent the violation; however, the bill provides no indication as to what actions would constitute due diligence. Furthermore, any relevant common law rule or principle that would create a justification or excuse may be relied on to the extent that it is not inconsistent with the Act.

The process for imposing liability under the AMP is a fairly expedited administrative process, administered through the CRTC. A notice may be served where the CRTC has reasonable grounds to believe that a person has committed a violation under the BILL C-28. The notice must include details of every act or omission for which the notice is served, the relevant provisions and the amount of the fine. The recipient of the notice has 30 days to respond, after which time he or she will be deemed to have committed the violation and will be liable to pay the amount set out in the notice. If the recipient does provide a response, the CRTC must decide on a balance of probabilities whether the violation was committed. Upon determining that there was a violation the CRTC may impose the original fine, impose a reduced fine, or may suspend payment of the fine subject to any conditions that it considers necessary to ensure compliance with the Act. Decisions of the CRTC can be appealed to the Federal Court of Appeal. However, where the issue is one of fact, leave to appeal must be granted by the Court. The CRTC can also agree to an undertaking, which is in essence an agreement to settle an alleged violation on terms acceptable to both the CRTC and the offender.

Private Right of Action

One of the most controversial provisions of Bill C-27 remains largely unchanged in Bill C-28. It would establish a private right of action for persons who allege that they have been affected by a contravention of the anti-spam, anti-phishing or anti-spyware provisions of Bill C-28. The application must include the alleged contravention, all relevant provisions, acts or omissions at issue, and should state the nature and amount of the loss, damage or expense. If the court is satisfied that the contravention occurred it may order the responsible individual(s) to pay the applicant compensation for any loss, damage or expenses incurred by the applicant. The court may also grant an additional award, up to a maximum of \$200 per day for most contraventions, and \$1 million for each day on which a contravention occurred. Again, officers, directors, or agents of corporations would be subject to this private right of action, if it could be proved that they directed, authorized or participated in the commission of the contravention.

That same private right of action would apply to persons who allege that they have been affected by breaches of the new provisions of *PIPEDA* and the *Competition Act*. These new provisions, discussed in detail below, would be brought into effect by Bill C-28.

Bill C-28 would also establish new anti-harvesting prohibitions under *PIPEDA* respecting the collection of personal information, including a ban on (i) collecting an individual's electronic address through a computer program designed or marketed for use in generating (or searching for) and collecting electronic addresses, or using any address collected by the foregoing means; and (ii) collecting personal information through any means of telecommunications if the collection involves accessing a computer system (or causing one to be accessed) without authorization, or using any personal information that is collected that way.

Bill C-28 also proposes numerous amendments to the *Competition Act*, including the addition of section 52.01, which would broaden the criminal false or misleading representation provisions of the *Competition Act*. This new section would prohibit knowingly or recklessly sending, for business promotion purposes: (i) a false or misleading representation in the sender or subject matter information of an electronic message; or (ii) an electronic message that contains a materially false or misleading representation. Under the proposed new section 74.011 of the *Competition Act*, such actions would also qualify as reviewable conduct, thus permitting the Commissioner of Competition to apply to a court or the Competition Tribunal for an order prohibiting the conduct and/or imposing AMPs under the *Competition Act*.

Impact on Telemarketing Rules

Bill C-28, if enacted, contains provisions that could, if proclaimed in force, amend the *Telecommunications Act* so as to replace the existing Do Not Call List (“DNCL”) regime with a new or modified scheme at a future date. The definition in Bill C-28 of “electronic message” is broad enough to encompass the voice and fax calls currently covered by the DNCL, meaning that the government might, at some future date, make these types of calls subject to the C-28 regime, signifying a transition to the “opt-in” approach of the new bill, as opposed to the “opt-out” regime contemplated with the DNCL.

Information Technology

FOCUS

Canadian tech company i4i takes on Microsoft

ARNOLD CEBALLOS

The United States Supreme Court is preparing to hear an important case with significant implications for patent holders, which pits a small Canadian company against software giant Microsoft Corporation. The case is so significant that dozens of amicus briefs have been filed on both sides of the case, with the U.S. government filing a brief supporting Toronto-based i4i Limited Partnership.

i4i sued Microsoft in 2007 for infringing a U.S. patent it holds on technology to open documents using the XML computer programming language. A Texas jury found in favour of i4i and ordered Microsoft to pay \$200 million in damages. A judge increased the damages award to \$290 million and ordered Microsoft to stop selling copies of its Word programs that could open certain files containing custom XML.

Microsoft unsuccessfully appealed to the Federal Circuit

Court of Appeals and then further appealed to the Supreme Court, which agreed to hear the case. Oral arguments are scheduled for April 18.

The legal issue the court will consider involves the standard to be considered when invalidating a patent, with i4i arguing that a higher "clear-and-convincing evidence" standard must apply, while Microsoft takes the position that a lower "preponderance of the evidence" standard should apply. At issue in the case was some prior technology that Microsoft believed called into question the validity of the patent and which the Patent Office did not review when granting the patent.

"This case is about the survival of a viable patent system in the United States," according to Loudon Owen, Chairman of i4i, who argued that patents need to be practically enforceable to encourage innovation and investment in new technologies. He noted that amicus briefs filed in support of i4i came from a range of parties from every

stage of the inventive process, from universities conducting research, to venture capitalists who seek to commercialize inventions, to large companies such as 3M Company and General Electric Company. In addition, the U.S. government has filed a brief in support of i4i, arguing that a higher standard for invalidating a patent reflects the proper deference to the authority of the Patent Office and its expertise, while also supporting the reliance interests of inventors.

In a written statement, Microsoft said that the case is about striking a proper balance. "The current approach taken by the Court of Appeals improperly tilts the scales to reward invalid patents," according to the statement from David Howard, Corporate Vice President and Deputy General Counsel for Litigation for Microsoft.

"That approach needs to be corrected in favour of a system that ensures the process for obtaining and defending patents is clear, reasonable and doesn't

unduly burden the system or innovation. When a patent issues, despite the fact that the Patent Office never had an opportunity to review the relevant prior technology, it enables the holders of those dubious patents to attack innovative companies with costly lawsuits. We believe a better balance will benefit all patent holders and innovators."

Microsoft has some significant allies as well, with amicus briefs filed in support of the company's position by companies such as Apple Inc. and Hewlett-Packard Co., as well as organizations such as the Business Software Alliance.

The United States Supreme Court may decide that invalidation of patents by clear and convincing evidence is not the standard in all cases, or is not the standard where new "prior art" is presented that was not before the Patent Office, according to Brian Gray, who practises intellectual property law with Ogilvy Renault LLP in Toronto. He added that many people believe that if the court grants the

appeal, it will become easier to invalidate U.S. patents.

"However, it is still questionable how much of an impact an esoteric legal standard will have on, for instance, a Texas jury, when faced with a U.S. patent issued by the U.S. government," noted Gray.

More importantly perhaps, said Gray, any decision has to be put in the context of the prevailing sentiment in the U.S. toward patent lawsuits with large jury damage awards.

This trend to restrict large jury awards includes court cases restricting the ability to obtain injunctions and choose favourable venues, as well as limiting damages by calling into question a 25 per cent rule of thumb for royalty calculations.

"These cases restricting patent damage recovery are likely to have much more of an impact than the i4i case," said Gray. ■



Gray

Anti-spam law governs software — not just email



DAVID ELDER

Think the new anti-spam law applies only to sending electronic messages? Think again.

Much has been written about how what has come to be known as Canada's Anti-Spam Legislation (CASL) will change the way that businesses communicate electronically, but the provisions in the legislation that govern the installation of "computer programs" seem to have received less attention — despite the fact that violators may find themselves exposed to injunctions, civil suits and administrative monetary penalties of up to \$10 million.

Any businesses that install or induce the installation of software, including those that distribute software for PCs or applications for devices such as smart phones, e-readers and tablet computers — or even those that operate websites — may want to review their practices in light of new disclosure and consent requirements contained in the statute.

The Act is intended to take aim at the covert installation of spyware and malware, such as the kind of programs that can transform PCs into "zombies" or bots that can be directed by third

parties to send out spam messages, but the statute casts a much wider net, capturing a wide array of commonly accepted commercial software and applications. Relying on the broad definition of "computer program" found in the *Criminal Code*, CASL applies to any set of instructions executed by a computer system and includes a wide range of downloadable material.

The legislation has broad territorial reach, applying where programs are downloaded to computers located in Canada, including by companies located outside of Canada; or are installed or caused to be installed by persons in Canada, or acting under the direction of a person in Canada, even if installed on computers outside Canada.

The law generally requires that no computer program must be installed without the prior consent of the owner or authorized user. In most cases, that consent must be explicit, and the party seeking consent must clearly describe the function and purpose of the program. It would appear that such consent could be obtained in a number of ways, including through installation pop-ups or user licence agreements. However, in all cases, the law would require some explicit affirmation, such as a click-through or signature.

More stringent disclosure and consent requirements apply where the program executes one

of several enumerated functions characterized as "beyond the reasonable expectations of the user," such as collecting personal information, changing user settings or preferences or communicating with another computer or device. While many of these functions are certainly hallmarks of malware and spyware, they may also be incorporated into what may be seen as more legitimate commercial applications, such as customer service software that may report usage and errors back to an enterprise, or media applications that may temporarily change user settings to optimize playback.

In such cases, the party seeking consent for the installation must describe the program's material elements, including their nature and purpose and their reasonably foreseeable impact on the operation of the computer system and must "bring those elements to the attention of" the user, suggesting notice beyond the description itself. The Act also states explicitly that this enhanced disclosure must be clear, prominent and separate from any licence agreement.

Significantly, the law applies not only to those installing programs directly, but also to those who may aid or induce the installation of a computer program without consent. Accordingly, operators of corporate websites should review all



MARCO RULKOTTER / DREAMSTIME.COM

"helper applications" that might be offered for download on or through their websites, such as special viewers or customer service applications, and ensure that the CASL disclosure and consent requirements are met.

Helpfully, the legislation deems consent to exist for the installation of certain types of common programs, where it is reasonable to believe from a user's conduct that they consent to the program's installation. Such "programs" include cookies, HTML code, Java scripts, operating systems or programs that are only executable through the use of another program, whose installation the user has previously consented to. The Act provides no elaboration on the circumstances in which it would be reasonable to assume consent, but a likely example would be the selection by a user of preferences in a browser for the acceptance of cookies.

While having received royal assent at the end of 2010, CASL has yet to be proclaimed in force. The government has announced its intention to first issue regulations, which may expand and clarify a number of the obligations in the legislation, including, potentially, the form and content of required disclosures and consent. The federal election call is expected to delay the publication of the proposed regulations and may therefore delay the law's originally expected coming into force in the fall of 2011.

Businesses should use this time to review their practices, process and user agreements and come into compliance. ■

David Elder is counsel with the Ottawa office of Stikeman Elliott LLP, where he practises communications, competition and privacy law.

LINKS

Decisions of Privacy Commissioners

PIPEDA Case Summary #2009-021:
http://www.priv.gc.ca/cf-dc/2009/2009_021_1223_e.cfm

PIPEDA Case Summary #2010-003:
http://www.priv.gc.ca/cf-dc/2010/2010_003_0928_e.cfm

Google Collects Personal Information from Wireless Networks:
http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm

PIPA Order P10-01 (British Columbia):
<http://www.oipc.bc.ca/PIPAOrders/2010/OrderP10-01.pdf>

Court Decisions

Stevens v. SNF Maritime Metals Inc. (2010 FC 1137):
<http://www.canlii.org/en/ca/fct/doc/2010/2010fc1137/2010fc1137.html>

Randall v. Nubodys Fitness Centres (2010 FC 681):
<http://www.canlii.org/en/ca/fct/doc/2010/2010fc681/2010fc681.html>

Compagnie d'assurances Standard Life c. Tremblay, 2010 QCCA 933:
<http://www.canlii.org/fr/qc/qcca/doc/2010/2010qcca933/2010qcca933.html>

Nammo v. Transunion of Canada Inc. (2010 FC 1284):
<http://www.canlii.org/en/ca/fct/doc/2010/2010fc1284/2010fc1284.html>

State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada (2010 FC 736): <http://www.canlii.org/en/ca/fct/doc/2010/2010fc736/2010fc736.html>

Mosher v. Coast Publishing Ltd., 2010 NSSC 153:
<http://www.canlii.org/en/ns/nssc/doc/2010/2010nssc153/2010nssc153.html>

Warman v. Wilkins-Fournier, [2010] ONSC 2126:
<http://www.canlii.org/en/on/onscdc/doc/2010/2010onsc2126/2010onsc2126.html>

Privacy Commissioner of Canada v. Air Canada (2010 FC 429):
<http://www.canlii.org/en/ca/fct/doc/2010/2010fc429/2010fc429.html>

Larose c. Banque Nationale du Canada (2010 QCCS 5385):
<http://www.canlii.org/fr/qc/qccs/doc/2010/2010qccs5385/2010qccs5385.html>

Citi Cards Canada v. Pleasance (2011 ONCA 3):
<http://www.canlii.org/en/on/onca/doc/2011/2011onca3/2011onca3.html>

R. v. Cole, (2011 ONCA 218):
<http://www.ontariocourts.on.ca/decisions/2011/2011ONCA0218.htm>

Jones v. Tsige (2011 ONSC 1475)
<http://www.canlii.org/en/on/onsc/doc/2011/2011onsc1475/2011onsc1475.html>

Guidance Documents

Data at Your Fingertips – Biometrics and the Challenges to Privacy (Released February 16, 2011):
http://www.priv.gc.ca/information/pub/gd_bio_201102_e.cfm

Fact Sheet: Privacy on the Go: 10 Tips for Individuals on Protecting Personal Information on Mobile Devices (Released January 24, 2011):
http://www.priv.gc.ca/fs-fi/02_05_d_47_dpd_e.cfm

Key Steps in Responding to Privacy Breaches (Released May 2010):
http://www.oipc.ab.ca/Content_Files/Files/Publications/Key_Steps_in_Responding_to_a_Privacy_Breach.pdf

Preparing for an Inquiry (Released in 2010):
http://www.oipc.ab.ca/Content_Files/Files/Publications/Preparing_for_an_Inquiry.pdf

Privacy Guidelines for Landlords and Tenants (Released 2010):
<http://www.oipc.bc.ca/pdfs/private/PrivacyGuidelinesforLandlordsandTenantsFINAL.pdf>

Instructions for Written Inquiries under the Personal Information Protection Act (Released June 2010):
http://www.oipc.bc.ca/pdfs/Policy/WrittenInstructions_PIPA_JUNE%202010.pdf

Aide mémoire à l'intention des citoyens: Perte ou vol de renseignements personnels: comment réagir? (Released May 2010):
http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Vol%20identite%20-%20citoyen%20-%2017%20mai%202010.pdf

Wall Street Journal Articles

"What They Know" series on digital privacy issues:
<http://online.wsj.com/public/page/what-they-know-digital-privacy.html>

SPAM AND PRIVACY UPDATE

Are you compliant?

FIRM PROFILE

An overview of Stikeman Elliott and our Technology, Intellectual Property and Communications Groups

SEMINAR WEDNESDAY, APRIL 13, 2011

Firm Profile

Stikeman Elliott LLP is one of Canada's leading business law firms, with offices in Toronto, Montreal, Ottawa, Calgary and Vancouver as well as in London, New York and Sydney. The firm is recognized as a Canadian leader in each of its core practice areas – corporate finance, M&A, corporate-commercial law, banking, structured finance, real estate, tax, insolvency, competition/antitrust, employment and business litigation – and is regularly retained by domestic and international companies in a wide range of industries including technology, financial services, telecommunication, insurance, transportation, manufacturing, mining, energy, infrastructure and retail.

“We wouldn’t get business done without them. They’re that good.”

Client Interview, IFLR1000

The firm’s Canadian offices are leaders in their respective jurisdictions and it has prominent cross-border expertise, as the first Canadian firm to open offices in London and New York, and extensive experience in the U.S., Europe, China, South and Southeast Asia as well as in Latin America, the Caribbean and Africa. Our 500 lawyers include many of Canada’s most prominent business practitioners and leading litigators, and our depth across practice areas enables clients to benefit from efficient, expert teams of lawyers at all levels. The firm has also invested heavily in leading-edge knowledge management and project management systems in order to assure our clients of advice of the highest quality.

Stikeman Elliott has been recognized by national and international legal directories as a Canadian leader in business law.

- > #1 for Lexpert/American Lawyer ranked lawyers in M&A, Corporate Finance and Corporate-Commercial
- > #1 for Lexpert ranked lawyers in M&A, Corporate Finance and Corporate-Commercial
- > #1 in the *Best Lawyers* rankings for M&A, Securities, Corporate Law and International Arbitration
- > Ranked Top-Tier in Corporate Law, M&A and Corporate Finance in Chambers Global’s *The World’s Leading Lawyers* and the International Financial Law Review *IFLR 1000*

The firm’s National Litigation Group, whose specializations include class actions, securities litigation, antitrust and restructurings, has been ranked among the top three business litigation practices in Canada by Lexpert. The firm is also well known for its extensive regulatory and government relations expertise; the latter anchored by its office in Ottawa.

Stikeman Elliott was named as one of Canada’s 50 Best Employers in 2010 and 2011 (as selected by Aon Hewitt), one of Canada’s Top 100 Employers from 2009-2011, one of Canada’s Best Diversity Employers and Best Employers for New Canadians for 2010 (each as selected by Mediacorp) and as one of Canada’s “Green 30” environmentally-friendly employers (as selected by Hewitt Associates, in partnership with Maclean’s and Canadian Business magazines). The firm was the first national Canadian law firm to be certified as carbon neutral, as of 2008.

Stikeman Elliott's Canadian offices are located in the major business and financial centres of Montréal, Toronto, Ottawa, Calgary, and Vancouver. Outside Canada, the firm's network includes offices or representation in the United Kingdom, the United States and the Asia-Pacific region. Our unsurpassed international experience ensures that we can serve our clients wherever their business takes them.



Montréal

The firm's Montréal office is one of the most successful and respected in the city. Its practice is focused on M&A, securities, banking, cross-border financial restructuring, international tax and commodity transactions, real estate, environmental law, intellectual property, information technology, transportation, insurance and employment law. The Montréal litigation group is widely recognized as one of the leading business law litigation teams in Quebec. Stikeman Elliott's expertise in civil law and commercial transactions is particularly significant where an organization has operations in Quebec or in other jurisdictions with codified civil law-based legal systems, such as Central and Eastern Europe and South America. Much of the work carried out in the Montréal office has a strong international focus.

Toronto

The Toronto office of Stikeman Elliott is a broadly based corporate-commercial law practice with a strong transactional focus. The firm's Toronto lawyers include many of Canada's foremost practitioners in the areas of M&A, securities, banking, structured finance, insolvency, tax, real estate, competition, employment, pensions, technology, outsourcing, mining and electricity law. The Toronto business litigation group is highly regarded for its record in commercial litigation, most notably securities litigation, class action defence and complex insolvencies and restructurings. The office is renowned for its expertise in cross-border transactional and litigation work and counts many major global corporations and financial institutions among its clients. The Toronto office has been recognized by local media as a top regional employer and one of the city's most environmentally-sustainable businesses.

Calgary

Our Calgary office, with currently more than 50 legal personnel, is home to some of Alberta's leading lawyers. The Calgary office opened in 1992 and maintains a business law practice focused on M&A, securities, real estate, joint ventures, project financings, structured financings, tax, employment and banking. The office also has a significant international dimension, advising on foreign investment in the Canadian energy sector and cross-border trade in energy resources. In addition, the office maintains a commercial litigation practice and is renowned for its regulatory practice involving oil and gas and electricity related matters. The Calgary office has recently won two awards for its active role in the community.

Vancouver

With over 22 years in the city, our Vancouver practice includes a number of British Columbia's leading lawyers in the areas of M&A, securities, banking, litigation and real estate. Our corporate lawyers lead local matters and draw on expertise of other Stikeman Elliott offices in national and international matters. We have one of British Columbia's most prominent real estate development and acquisition practices, while our Litigation Group has acted for all levels of government and offers a broad range of commercial dispute resolution and advocacy services, including significant class action expertise. A very experienced group of lawyers also practice in the areas of public-private partnerships, infrastructure development and project finance. The Vancouver office has a strong cross-border focus, acting as the firm's Canadian gateway to the Asia-Pacific region.

Ottawa

The Ottawa office of Stikeman Elliott focuses on administrative law and regulated industries, with particular emphasis on competition law, intellectual property law, international trade, government procurement and public policy. Industry sectors in which the office has expertise include such federally-regulated commercial sectors as telecommunications, broadcasting, transportation, and energy, as well as those (such as packaging and labelling) that are subject to food and drug administration.

London

Drawing on over 40 years of experience in the city, Stikeman Elliott's London office has long been recognized for its leadership in international corporate transactions, including leveraged buy-outs, take-over bids and share and asset purchases. Our London corporate finance team is a leading advisor to Canadian companies with respect to Toronto Stock Exchange and AIM listings and has been recognized for many years as one of the most prominent international advisors in the Eurobond markets. We have also been at the forefront of developing the legal framework for the issuance of Maple Bonds in Canada. Our lawyers have broad industry expertise, as well as significant experience in Africa, in the mining sector. The office also serves as the gateway for our India, Middle East and Sovereign Wealth Fund practices. As well, our private client practice ranks amongst the world's leading practices in the area.

New York

The New York office of Stikeman Elliott has extensive experience in Canada-U.S. cross-border corporate transactions, with a particular focus on M&A, corporate finance, banking and structured finance. The firm's New York lawyers provide Canadian legal advice on cross-border acquisitions, investments, banking, securities and regulatory matters to U.S. corporations, investment dealers, advisors, banks and funds.

Sydney

Stikeman Elliott's Sydney office, the hub of our Asia-Pacific practice, is involved in multi-jurisdictional securities and M&A law with a sectoral emphasis on mining, cross border M&A, infrastructure development and project finance.

Asia

Stikeman Elliott regularly acts in transactions involving clients across Asia, including, in particular, India, China, Hong Kong, Thailand and the Middle East. Reflecting the position of Canada as a target for a rapidly expanding Asian region and as a significant source of capital, the firm provides advice on a large number of significant transactions from Asia into Canada, as well as advising on Canadian investment into Asia. The firm has a particularly high profile in resource-sector transactions and is involved in the vast majority of IPOs originating in Asia that involve placements into Canada.

Technology

The Stikeman Elliott Technology Group understands its clients' business challenges and the unique role and risks associated with the exploitation of information technology, combining this understanding with sophisticated corporate capabilities to deliver the best possible support for any technology-related matter. The Stikeman Elliott Technology Group is comprised of technology practitioners who are fully integrated into the firm's transactional business law practice, ensuring that the members have strong corporate-commercial skills to complement their significant technology expertise. This multidisciplinary approach combined with the group's depth of transaction experience allows the group to provide innovative, practical legal advice for complex technology arrangements.

The Stikeman Elliott technology lawyers with whom you would be working understand both the business and the technology drivers of technology contracting, a product of experience that – in addition to the mandates described below – includes negotiating with virtually all of the major technology service providers, software companies and hardware manufacturers, including SAP, Oracle, Sun, IBM, CGI, EDS, Microsoft, Cognos, Manugistics, Entrust and HP.

The core competencies of the Technology Group are:

Service Arrangements and Outsourcing

Members of our Technology Group have assisted clients with the negotiation and drafting of some of the most complex service and outsourcing transactions in Canada, including a wide range of offshore outsourcing transactions, cross border outsourcings into Canada and federal and provincial government procurement transactions.

Licensing and Commercialization

Stikeman Elliott has in-depth experience negotiating and drafting technology, patent and other intellectual property licensing, exploitation and commercialization agreements. We regularly represent both vendors and customers, advising on all aspects involving the licensing, exploitation or commercialization of intellectual property.

Technology Development

The protection and allocation of ownership rights in intellectual property is often complicated and contentious in the context of technology development, particularly where developed technology contains or relies upon pre-existing or underlying technology. Members of the Technology Group have significant experience advising on the issues arising out of development, design and manufacturing arrangements involving technology.

Privacy

Stikeman Elliott is highly regarded for innovative solutions to the challenges presented by the privacy and data protection laws in Canada. Members of our Technology Group help clients understand these laws and advise them on developing compliant practices and programs.

Intellectual Property Management / Branding

Members of the group are frequently called upon to assist clients in respect of critical intellectual property and branding issues as they relate to technology, including patent portfolio development and enforcement, confidentiality, copyright issues (particularly as they

relate to software), employee intellectual property issues, trade-marks, domain names, and the protection of corporate and brand identities, as well as other aspects of the protection and exploitation of technology.

Technology Litigation

Members of the Technology Group advise clients with respect to software/licence disputes, patent infringement and validity matters, copyright and industrial design disputes, trade secrets, passing off and confidential information, valuation disputes in the IT field, departing employee disputes and related injunctions, obtaining Anton Pillar orders with respect to trade secrets, confidential information and proprietary technology, product liability and deficiency cases, and financing issues and disputes.

E-commerce and Internet Infrastructure

Stikeman Elliott has experience in enabling clients to do business electronically and over the Internet, including advising on issues relating to electronic contracting, website development or hosting agreements and B2B marketplaces.

Intellectual Property

As new ideas promise to drive today's changing economy, strategic use and care of the intellectual property of your business is a key factor in success and risk management. While intellectual property is especially vital for high-technology firms, its importance cuts across industry sectors as well as national boundaries. Businesses have a growing need for innovative legal advisers in Canada and around the world to help them exploit their intellectual property to the fullest extent and in as many markets as possible while reducing the risks of that exploitation.

Because intellectual property issues arise in a wide variety of contexts, Stikeman Elliott takes a multi-disciplinary approach to the practice of intellectual property law. Our Intellectual Property Group is composed of a team of dynamic and highly creative professionals who bring a wide range of training and experience in corporate-commercial law, banking & financial services, technology and outsourcing, as well as expertise with a wide variety of industry sectors.

Among the areas in which Stikeman Elliott provides intellectual property expertise and assistance are:

- > **Corporate transactions: Licensing, Co-branding and Outsourcing** – The firm represents clients in a variety of corporate transactions with specific intellectual property implications, such as licensing, co-branding, outsourcing and distribution arrangements. We also provide intellectual property advice in public offerings, joint ventures, mergers, acquisitions and divestitures when rights are at issue. The Intellectual Property Group works with corporate, tax, trade and other lawyers to evaluate intellectual property aspects of corporate transactions, such as carrying out intellectual property due diligence searches in corporate acquisitions and assisting clients throughout the transfer of technology process. We have acted in a number of co-branding transactions in financial services and credit card sectors, as well as other retail merchandise and consumer goods.
- > **Acquisition, protection and exploitation of intellectual property rights, in Canada and abroad** – Stikeman Elliott counsels Canadian and foreign clients on the manner in which they may protect their intellectual property, acquire the intellectual property of others and best exploit their intellectual property portfolio. We also regularly advise clients and draft agreements on the franchising, licensing and assignment of intellectual property rights in a wide variety of contexts, including character licensing, as well as agreements respecting merchandising, sponsorship, and use of intellectual property as security.
- > **Registration of trade-marks, patents, industrial designs and copyrights** – We regularly file Canadian trade-mark, patent, industrial design and copyright applications on behalf of clients and assists in filing similar applications applied for in other countries;
- > **Intellectual property litigation** – Stikeman Elliott represents clients in all areas of intellectual property litigation, including trade-mark, patent, industrial designs or copyright infringement actions before Canadian courts and proceedings before administrative tribunals such as the Trade-marks Opposition Board, the Copyright Board and the Patent Medicine Prices Review Board;

- > **Intellectual property on the Internet** – We represent clients with respect to a variety of Internet matters and we advise on the protection of intellectual property rights, freedom of speech, the implications of the application of new audio-visual technologies to the Internet, gambling on the Internet, and the applicability of Canada’s collective copyright regime to copyrighted works accessible on the Internet.
- > **Trade secrets and confidential information** – Our lawyers regularly advise clients on how to protect trade secrets and confidential information in a variety of situations, including with respect to contracting out of services, departing employees and joint ventures, and also acts on behalf of clients in trade secrets litigation.
- > **Intellectual property issues in the pharmaceutical and healthcare industry** – Stikeman Elliott has cultivated strong relationships with health sector regulators and can assist clients in navigating the complex regulatory approval process for pharmaceutical and healthcare products, including regulatory approval from Health Canada and other government agencies on new drug submissions, labelling, good manufacturing practices, recall procedures and non-prescription drugs.
- > **Entertainment and cultural industries.** The Group has worked with a variety of clients in such diverse entertainment and cultural areas as endorsements, print, music and audiovisual publishing and performance, telecommunications, and multimedia productions.
- > **Public Policy and Advocacy.** Clients frequently consult Stikeman Elliott to assist them in monitoring, understanding and influencing ongoing policy developments in a number of intellectual property areas.

Communications

Stikeman Elliott's Communications Group consists of partners and associates drawn from the firm's domestic and international law offices possessing expertise in telecommunications and broadcasting law and complementary legal disciplines, including competition, corporate and commercial, and copyright. The Group is able to draw upon the particular strengths of each of its members in responding to clients' needs. This ensures that our clients receive legal services tailored to their specific needs in a timely and cost-effective manner, regardless of the complexity of the issues or the size of the particular transaction. The Group has established a blog on legal, legislative and policy developments that can be accessed online at www.CanadianCommunicationsLaw.com.

Background

Prior to joining Stikeman Elliott, members of the Communications Group gained valuable experience working in a variety of capacities, including senior positions at the Canadian Radio-television and Telecommunications Commission (CRTC) and in senior executive positions for companies in the regulated communications sector in Canada. They remain on the leading edge of new technology and legal issues through regular appearances before the CRTC, Industry Canada, the Supreme Court of Canada, the Federal Court of Appeal, as well as research and writing, participation in conferences and teaching at universities. All of this enables the members of the Group to keep pace with the rapid developments and innovations that are characteristic of the telecommunications and broadcasting sectors in Canada and abroad.

Given Government policy that directs the CRTC to rely on market forces to the maximum extent feasible, we consider the Communications Group should include knowledge and experience with respect to the past and current administration of the *Telecommunications Act* and related regulations as well as the *Competition Act*. In our view a practice group should also provide a range of expertise and seniority that permits work to be done at the most appropriate level of experience and billing rate.

Experience

More specifically, the Group possesses a wide and varied experience with respect to domestic and international telecommunications and broadcasting law activities. The communications sector in Canada is still subject to a significant degree of regulation. Members of the Communications Group at Stikeman Elliott have a breadth of experience relating to the principal regulatory forums including the CRTC, the Competition Bureau, the Departments of Industry Canada and Canadian Heritage as well as the Federal and Supreme Courts of Canada in judicial review and appeal activities. While we have acted principally for private sector clients, we have also been retained by government agencies and organizations in Canada and abroad.

Our Services

Telecommunications

Members of the Group have acted as counsel and have provided advice of both a general and a more specific nature to a number of telecommunications common carriers (terrestrial, wireless and satellite), resellers, Internet Service Providers and content providers and users. Our experience includes the following:

- > Relative to the CRTC, members of our Group have appeared as counsel in regulatory proceedings pursuant to the *Telecommunications Act* such as rate and service applications, applications for entry, licensing, the provision of competitive domestic and international telecommunications services including resale and sharing applications for forbearance from regulation, Canadian ownership and control, competitive disputes, as well as consideration of CRTC jurisdiction respecting the Internet and Internet Service Providers; and
- > Relative to Industry Canada, we have acted as counsel in the context of major licensing initiatives and transfers of licences pursuant to the *Radiocommunication Act* including domestic and global satellite services, wireless services including cellular telephone, paging, public cordless telephone service, policy proceedings to define licensing criteria for new services, the Telecommunications Policy Review, foreign ownership issues and proceedings which culminated in the drafting of new legislation and regulations.

Broadcasting, Specialty Services and Broadcasting Distribution

Although Canada is experiencing convergence, broadcasting communications matters are regulated by the CRTC separate from telecommunications under the administration of the *Broadcasting Act* and the establishment of policy by the Government through the Department of Canadian Heritage. Experience with respect to the broadcasting sector has included the following:

- > Relative to the CRTC, acting on behalf of clients in a wide variety of proceedings including licensing of radio, television and specialty undertakings, cable television, satellite and other wireless broadcasting distribution undertaking activities, authority for the transfer of licences as a result of acquisitions or mergers, foreign ownership issues, licence renewals, competitive disputes and policy proceedings as well as CRTC jurisdiction with respect to conventional and new media services relative to Internet distribution;
- > In the CRTC proceedings described above, we have acted on behalf of applicants for licences to be issued by the CRTC, as well as interested parties in interventions either supporting or opposing applications filed by others; and
- > Relative to major acquisitions and financings of companies in this regulated sector, we have provided comprehensive legal advice to the companies involved and financial institutions.

Copyright

Leveraging the firm's intellectual property expertise, the Group has acted on behalf of a range of clients respecting legislative developments in the area of copyright, applications for approval of tariffs for the collective administration of copyright and court challenges respecting decisions of the Copyright Board of Canada.

Mergers and Acquisitions

Drawing upon the strengths inherent in a team approach, lawyers in the Group have provided the regulatory component in major corporate transactions. This has included securing regulatory approvals where required and guidance with respect to limitations on foreign ownership in both the telecommunications and broadcasting sectors.

International

Stikeman Elliott has provided counsel to private sector clients and to a number of governments and administrations as a result of the World Trade Organization Agreement on Basic Telecommunications. Some of the countries and administrations include: Italy, Belgium, Hungary, Romania, South Africa, India, Pakistan, Bangladesh, Chile, Solomon Islands and the Bahamas.

Legislation

Members of our Group have advised government departments and private sector clients in the drafting of legislation and legislative amendments with respect to the *Telecommunications Act*, the *Broadcasting Act*, the *Radiocommunication Act*, the *Telesat Canada Act*, and the *Teleglobe Canada Reorganization and Divestiture Act*.

Privatization

There have been significant privatization activities in Canada regarding the telecommunications sector and Stikeman Elliott has acted for the Canadian Government as vendor, for a Crown Corporation being privatized, and for potential purchasers of companies being privatized. The Communications Group, in association with other relevant practice groups in the firm, has provided wide-ranging advice and legal services to both structure and execute the privatization mandates. This includes advice on securities and financial aspects through to the policy and legislative drafting required to complete the privatization. In addition, with the benefit of experience gained in the Canadian context, the relevant practice groups in Stikeman Elliott have also provided advice on privatization activities in other jurisdictions.

Lawful Access

Members of our Group have been key players in the development in Canada of legislation requiring telecommunications carriers to build and maintain capability to provide lawful access to telecommunications and related data by law enforcement and national security agencies, and have advised a variety of clients with respect to compliance with lawful access requirements.

Unsolicited Telecommunications

Canada has long had rules respecting the use of telecommunications technologies for marketing, informational and charitable purposes, including Unsolicited Telecommunications Rules, a National Do Not Call List, and most recently, broad-based anti-spam legislation. Lawyers in the Communications Group have assisted a variety of clients in navigating the complexities of these rules and their enforcement.

Recognition for Our Work

Our Communications Group is noted in *Chambers Global 2011* as a leading law firm in the telecommunications industry, and further noted as a “respected group, praised for its regulatory capacity in both telecoms and broadcasting,” and for its involvement “in a number of high-profile mandates, including acting for Shaw Communications on jurisdictional questions concerning the CRTC before the Federal Court of Appeal.” Members of the Group

have been recognized and cited by a variety of domestic and international directories, such as *Chambers Global: Guide to the World's Leading Lawyers for Business* and *Guide to the World's Leading Telecommunications Lawyers*, *The International Who's Who of Regulatory Communications Lawyers*, *The Best of the Best*, *Lexpert's Guide to the Leading 500 Lawyers in Canada*, *The Canadian Legal Lexpert Directory*, *PLC Which Lawyer?*, *The Best Lawyers in Canada*, *PLC Cross-border Media & Communications Handbook*, and *The Telecommunications Law Guide*.

Among our Group members are:

- > **Gregory Kane, QC**, the head of the Group, has been cited as a Canadian leader in the sector by *Chambers Global*: “He has terrific judgment and really knows his stuff,’ say sources, while others laud his years of experience. He acts for clients in copyright, regulatory, satellite and privatization matters in front of the CRTC, Industry Canada and Canadian Heritage.” Sources note he is “fantastic – a key player in CRTC regulatory work’ and [h]e’s the star of the show and a real old-school gentleman”.
- > **Lawson Hunter, QC** is a former Executive Vice-President and Chief Corporate Officer of Bell Canada and BCE Inc., where he was responsible for overseeing regulatory, governmental relations and corporate affairs. He is also a former Commissioner of Competition. Mr. Hunter is recognized as a world leader in competition/antitrust law and telecommunications.
- > **Nicholas McHaffie** is head of the litigation group in Stikeman Elliott’s Ottawa office. His practice includes both regulatory and intellectual property aspects of telecommunications and broadcasting. He has represented clients before the Federal Court of Canada, the Federal Court of Appeal and the Supreme Court of Canada on telecommunications and broadcasting matters, including recent experience on the CRTC’s reference regarding the status of ISPs under the *Broadcasting Act*. He has also acted for clients before the Copyright Board and Federal Court of Appeal in tariff proceedings under the *Copyright Act*.
- > **David Elder** is a former Legal Counsel to the CRTC and Vice President, Regulatory Law with Bell Canada, where his practice and managerial responsibilities dealt with a wide variety of matters relating to the regulation of broadcasting and telecommunications in Canada, as well as developments in the areas of privacy, security, lawful access to private communications, electronic commerce and new media. He also acted as Bell Privacy Ombudsman and Senior Regulatory Counsel to Bell ExpressVu (now BellTV). David is recognized by *Chambers Global* as being “highly recommended for his substantial knowledge of telecoms, broadcasting, privacy and lawful access issues.”
- > **Paul Beaudry** is a former senior policy advisor to a federal Minister of Industry Canada and contributed to two landmark government decisions that modernized telecommunications regulatory framework and accelerated de-regulation of local telephony.
- > **Stuart McCormack** is head of the Intellectual Property Group and has led appearances before the Copyright Board of Canada on matters relating to, among other things, retransmission royalties payable by cable companies, the jurisdiction of the Board over internet television “broadcasting,” and levies payable on blank recording media.

Stikeman Elliott's COMMUNICATIONS LAW BLOG

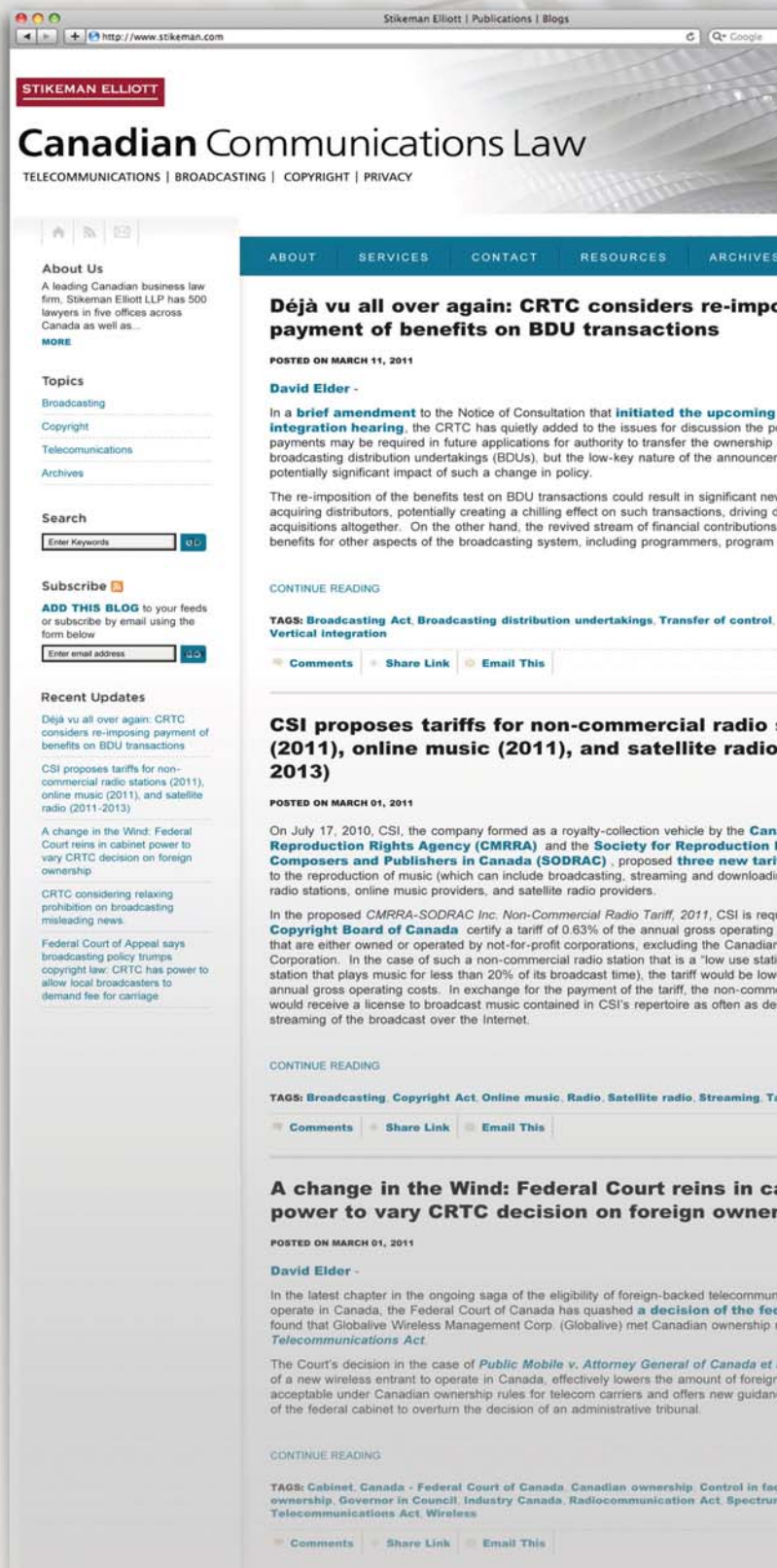
CanadianCommunicationsLaw.com

Canada's New Online Resource for Communications Law Developments and Analysis

- **Featuring information and commentary** on relevant legal, legislative and policy developments including:
 - Radio and television broadcasting
 - Cable and satellite distribution
 - New media and internet content
 - Broadcasting and internet copyright issues
 - Wireline telecommunications
 - Wireless telecommunications and spectrum licensing
 - Convergence issues
 - Competition in broadcasting and telecommunications markets
 - Transfers of ownership and Canadian ownership requirements
 - Unsolicited telecommunications, Do Not Call List and anti-spam requirements
- **Fully searchable** with archived materials, indexed by topic
- **Subscribe** for immediate updates via e-mail or RSS feed

Check out the site at:
www.CanadianCommunicationsLaw.com

Also check out Stikeman Elliott's other blogs at
blogs.stikeman.com



Stikeman Elliott's TECHNOLOGY & IP BLOG

CanadianTechnologyIPLaw.com

Canada's New Online Resource for Technology & IP Law Developments and Analysis

- **Real-time information and commentary** on relevant legal developments including:
 - outsourcing
 - e-commerce
 - corporate transactions
 - privacy
- Fully searchable with extensive archived materials, indexed by topic
- Subscribe for immediate updates via e-mail or RSS feed

Check out the site at:
www.CanadianTechnologyIPLaw.com

Also check out Stikeman Elliott's other blogs at blogs.stikeman.com

The screenshot shows the website interface for Stikeman Elliott's Canadian Technology & IP Law blog. The header includes the firm's name and the blog title. The main content area features a list of recent updates and a detailed article titled "Privacy Commissioner can now be choosier about complaints she investigates". The article text discusses legislative amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) and mentions the Privacy Commissioner's new role in selecting complaints for investigation. The article is dated April 4, 2011, and is written by David Elder. The interface also includes navigation menus, a search bar, and social media links.

MONTRÉAL

1155 René-Lévesque Blvd. West, 40th Floor, Montréal, QC, Canada H3B 3V2
Tel: (514) 397-3000 Fax: (514) 397-3222

TORONTO

5300 Commerce Court West, 199 Bay Street, Toronto, ON, Canada M5L 1B9
Tel: (416) 869-5500 Fax: (416) 947-0866

OTTAWA

Suite 1600, 50 O'Connor Street, Ottawa, ON, Canada K1P 6L2
Tel: (613) 234-4555 Fax: (613) 230-8877

CALGARY

4300 Bankers Hall West, 888 - 3rd Street S.W., Calgary, AB, Canada T2P 5C5
Tel: (403) 266-9000 Fax: (403) 266-9034

VANCOUVER

Suite 1700, Park Place, 666 Burrard Street, Vancouver, BC, Canada V6C 2X8
Tel: (604) 631-1300 Fax: (604) 681-1825

NEW YORK

445 Park Avenue, 7th Floor, New York, NY 10022
Tel: (212) 371-8855 Fax: (212) 371-7087

LONDON

Dauntsey House, 4B Frederick's Place, London EC2R 8AB England
Tel: 44 20 7367 0150 Fax: 44 20 7367 0160

SYDNEY

Level 12, The Chifley Tower, 2 Chifley Square, Sydney N.S.W. 2000 Australia
Tel: (61-2) 9232 7199 Fax: (61-2) 9232 6908