TOP 10
LEGAL RISKS FOR BUSINESS
IN 2016

BLG
Borden Ladner Gervais
It begins with service

CLIMATE CHANGE

TAX AUTHORITIES

PRIVACY CLASS ACTIONS

WORKPLACE IT SECURITY

FRAUD IN E-PAYMENT SYSTEMS

REGULATORY PURGATORY

HONESTY IN LAW CONTRACTS

TRANS-PACIFIC PARTNERSHIP

COMPLIANCE

CASL

TOP 10 LEGAL RISKS FOR BUSINESS IN 2016

BLG's Top 10 Legal Risks for Business in 2016 is our annual thought leadership report forecasting the key trends and regulatory changes that will have legal implications for our clients in the year ahead.

blg.com/top10

About Borden Ladner Gervais LLP

Borden Ladner Gervais LLP (BLG) is a leading, national, full-service Canadian law firm focusing on business law, commercial litigation and arbitration, and intellectual property solutions for our clients. BLG is one of the country's largest law firms with more than 725 lawyers, intellectual property agents and other professionals in five cities across Canada. We assist clients with their legal needs, from major litigation to financing to trademark and patent registration.

Climate Change

Canada's greenhouse gas regime is poised to be one of the country's leading business challenges in 2016. From Paris to provincial legislatures, big changes are coming, with Canadian companies – and large carbon emitters across a range of industries – still determining what the impacts will be on their bottom lines.

Nationally, there will be significant changes to Canada's energy systems and economy, heavily weighted in natural resources. With green energy sources likely to play a larger role, experienced renewable project developers with strong balance sheets and a low cost of capital are likely to be some of the biggest winners in 2016.

In Alberta, Premier Rachel Notley announced a far-reaching and comprehensive climate change strategy, with sweeping new regulatory requirements for the electricity, oil and gas industries. The result for a province already reeling from low commodity prices is an economy-wide carbon tax, a 100 megatonne cap on oil sands emissions and a phase-out of coal. Ontario has proposed a cap and trade program, to take effect in 2016, which will be its primary vehicle to achieve emissions targets. Depending upon the industry, new policies in Edmonton and Ontario may reflect an operational cost, a barrier to entry or a reason to shut down entirely.

Companies with emissions-reducing technologies, or venture capital/private equity focused on renewable and energy efficiency project financing are currently well-placed for success. However, even outside of Alberta, de-carbonization and structural changes to the oil and gas industry will have significant commercial implications, for example, on manufacturers in Central Canada, large energy consumers and overall currency valuation.

In the upcoming year, business will look ahead to not only the implementation of provincial carbon initiatives, but also to the federal government pursuing its own climate change agenda. This involves new international obligations arising from the 2015 United Nations Climate Change Conference, as well as a commitment to set national emissions targets. 2016 will therefore be a watershed year for Canadian business in navigating the shoals of carbon policy and economic transition. Changes are expected to be rapid and multi-dimensional, effects complicated.

Alan Ross
aross@blg.com

Marie-Claude Bellemare
mbellemare@blg.com

Government of Canada to endow a $2 BILLION LOW CARBON ECONOMY TRUST to fund projects that reduce carbon.[1]

THE RATE OF GLOBAL WARMING OVER THE LAST 50 YEARS is almost DOUBLE the rate of warming over the last 100 YEARS.

Worldwide 14 of the last 15 years have been the warmest on record.[2]

Tax Authorities Continue to Pursue Non-privileged Information

Canadian tax authorities continue to aggressively pursue taxpayer information, using the extensive powers granted to them under tax legislation. Sensitive communications with, and work product prepared by, accountants and other non-lawyers represent fertile ground for the Canada Revenue Agency. This was illustrated by the CRA's success before the Federal Court of Canada in *Minister of National Revenue v. BP Canada Energy Company*, in June 2015, in forcing disclosure of the taxpayer's list of uncertain tax positions prepared for financial statement purposes, for use as an "audit roadmap." Governments' need for tax revenues and the global trend towards greater tax transparency will only make revenue authorities more aggressive in seeking confidential information. Lawyer-client privilege constitutes the one defence to information demands that Canadian courts have consistently upheld, and well-advised taxpayers will ensure that tax-sensitive communications and work product are prepared on a privileged basis to the greatest extent possible.

Steve Suarez
ssuarez@blg.com

Charles Marquette
cmarquette@blg.com

For the period April 1, 2006 to March 31, 2014, the CRA CONVICTED 1,508 TAXPAYERS.

This involved approximately $223 MILLION in federal tax evaded and court sentences totalling $118 MILLION in court fines and 4,692 MONTHS of jail time.[3]

Privacy Class Actions are on the Rise in Canada

There is a new trend in Canada towards privacy class actions being launched following a cybersecurity breach or an improper disclosure of personal information. Indeed, privacy class actions triggered by data breaches are growing in popularity in Canada, with between twenty and thirty privacy class actions currently pending or already certified. These lawsuits follow either a cybersecurity or another similar data security breach, or the launch of a new privacy-sensitive product or innovative marketing program.

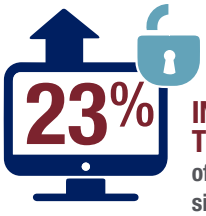
On the data security front, businesses, particularly small to mid-size entities, often lack breach response policies, proper governance tools, and employee privacy training programs to prevent or promptly respond to breaches. They lack cybersecurity preparedness, which makes them vulnerable to privacy class actions following a security breach involving personal information.

On the privacy front, many businesses have recently received bad press because of new advertising programs, online business models and services. Canadian businesses have been capturing and analyzing large amounts of data for years and they are now at the point where they want to use this data. For instance, they are looking to sell analytic tools allowing others to obtain more insights into their (actual or potential) customers or to provide more personalized products, services or advertising, both online (i.e. mobile) and offline, sometimes even using location data.

In the era of Big Data, new business models and marketing techniques are emerging, including facial recognition and personalization reaching new levels of sophistication, as well as dynamic pricing practices, to name but a few. Businesses need to consider whether personal information is properly "de-identified", what type of information should be considered as "sensitive" in various contexts (security breaches, targeted advertising, online services, etc.), how to obtain valid consent in compliance with the "reasonable expectations" of customers, and how to deal with technological innovation, shifting social norms, and building customer trust through proper privacy practices. With new innovative technologies (Internet of things, health bracelets and wearables, to name just a few), and new business models on the rise, businesses have to ensure that their practices are legally compliant, as well as ethical, fair, and reasonable.

Ira Nishisato
inishisato@blg.com

Éloïse Gratton
egratton@blg.com



INCREASE IN TOTAL COST
of data breach since 2013.[4]

$3.79 MILLION

AVERAGE TOTAL COST
of each data breach.[5]

Class actions remain the **preferable option** for privacy enforcement.[6]

Workplace Cyber-Sex and IT Security

2015 saw a number of high-profile cyber-sex security breaches. Most prominent was the Ashley Madison scandal, in which the personal details of over 37 million people were exposed through the hacking of a website that encourages and facilitates extramarital affairs. Worryingly for employers, many subscribers to the website had signed up using their professional e-mail accounts. Other examples, such as Snapchat or Netflix, are less unsavoury, but they may be equally disruptive and potentially dangerous to an employer's interests: apart from the potential loss of reputation, such behaviour puts the integrity of the security systems implemented by employers at risk.

More and more, the lines between work and personal technologies become blurred, so that many employees no longer make a conscious distinction between work email addresses and personal ones. Employers are strongly encouraged to elaborate on IT security systems in place, as well as policies describing the appropriate use of the company's network and the professional email accounts linked thereto. However, in the face of these deliberate breaches by employees, who may not even be aware that they are breaching the employer's policy, let alone realise that their transgressions may cause harm, many employers wonder what they can do to limit their exposure caused by such behaviour.

Jason Howg
jhowg@blg.com

Matthew Certosimo
mcertosimo@blg.com

Justine Laurier
jlaurier@blg.com

While **employees** remain the most cited source of compromise, incidents attributed to business partners climbed 22%.[7]

Ashley Madison hack: A substantial number of addresses from **various Fortune 500 companies** like Microsoft MSFT +0.00%, Cisco, Apple, and Bank of America.[8]

Combatting Fraud in e-Payment Systems

The advent of mobile and digital wallets coupled with contactless payment methods and the ever-increasing growth in on-line payments have made e-payments become ubiquitous and have increased the need to develop effective authentication protocols, technology, policies and procedures to mitigate and reduce the risk of fraud. Recent legal cases in the United States have allowed negligence claims against financial institutions that do not have effective multi-factor authentication systems in place, where losses would otherwise have been borne by customers. As technology develops and consumer transactions and instructions are increasingly provided remotely or through contactless methods, effective authentication and security technology will continue to become increasingly critical. The use of digital wallets requires careful review of financial services account agreements; in particular limitations of liability and other provisions relating to allocation of risk ought to be reviewed. As with debit cards, financial institutions should expect losses may be borne by them, except where the consumer does not cooperate with an investigation, fails to report a lost or stolen card or fails to protect his or her PIN.

Stephen Redican
sredican@blg.com

Éloïse Gratton
egratton@blg.com

IN 2015, EVERY **$100** OF FRAUD, COSTS A MERCHANT **$223.**[9]

Up to **7X** MORE DIFFICULT TO PREVENT FRAUD in remote channels than in person.[10]

In 2015, debit card-accepting merchants attributed **30% OF FRAUD** to this payment type.[11]

Regulatory Purgatory will Impact Business Decisions

Canada's securities regulatory system has always been slow to effect harmonized changes to securities regulation. However, in 2016, we expect that certain initiatives which have taken a long time to enact will impact Canadian public companies. Defensive tactics by target companies in the face of hostile takeover bids, and particularly discussions about "poison pills", have again hit the headlines. The proposed takeover bid regime announced by the CSA in March 2015, which will have a practical effect on defensive tactics such as poison pills, has yet to be finalized. This is making it difficult for parties involved in hostile bid transactions, as bidders must comply with the existing takeover rules, while targets implement defensive tactics based on the proposed regime that is not yet in force and which may yet be subject to change. At a time when markets are in flux (particularly for those industries affected by commodity price uncertainty) the addition of regulatory uncertainty may result in fewer hostile transactions and in circumstances where defensive tactics are challenged, may result in *ad hoc* decisions by securities regulators that in turn will add uncertainty. In addition, the administration of securities regulation is poised to change with the advent of the Cooperative Capital Market Regulatory System (CCMRS). Should the CCMRS become operational in 2016, the changes brought by the CCMRS will start to impact businesses, as they struggle to understand how the new "harmonized" system will affect them and, in particular, will likely result in regulatory delay, as the various securities regulators find their footing in establishing a new working relationship with each other.

Gordon Raman
graman@blg.com

Pascal de Guise
pdeguise@blg.com

Kent Kufeldt
kkufeldt@blg.com

A new national framework proposed for the regulation of takeover bids, including the use of "**poison pills**" by target companies. [12]

Takeover bids must receive tenders of **MORE THAN 50%** of the outstanding securities subject to the bid. [13]

Bids must remain open for a **MINIMUM OF 120 DAYS** – a significant increase from the current requirements of **35 DAYS.** [14]

Honesty is No Longer the Best Policy – It's the Law in Contracts

In *Bhasin v Hrynew* released in November 2014, the Supreme Court of Canada recognized a new duty for contracting parties: the "honest performance" of contractual obligations. Pursuant to this new duty, "parties must not lie or otherwise knowingly mislead each other about matters directly linked to the performance of a contract". The Court does not see this as imposing a positive duty of disclosure: it distinguishes between "active dishonesty", which is not permitted, and failure to disclose a material fact, which appears to be.

The Court also recognized for the first time in Canadian common law that there is a "general organizing principle" of good faith contractual performance. Pursuant to this principle, "parties generally must perform their contractual duties honestly and reasonably and not capriciously or arbitrarily".

While parties to a contract cannot contract out of "honest performance", the Court held that the content of the duty and standards for satisfying it may be defined in an agreement, as long as the parties respect the duty's "minimum core requirements".

While the decision was an attempt to provide some certainty and predictability in an area which has to date been inconsistent and unclear in Canada (outside of Québec), the decision leaves a number of questions open: How will the new duty of honest performance be measured? What are its "minimum core requirements"? Is it a free-standing cause of action? How will damages be assessed? Will other new duties be recognized under the newly-recognized organizing principle of good faith performance? Another open question is how the decision will be applied to pre-contractual dealings, such as negotiations.

With "honest performance" comes a new area of litigation and now businesses must actively consider whether they are discharging the new duty when performing under a contract. If a given course of action may be construed as actively dishonest, misleading, or not forthright, businesses should avoid pursuing such course of action unless they are prepared to accept the risks and consequences of litigation. As claims for breaches continue to grow in Canadian courts, all businesses should be aware of their duty of good faith in the performance of their contractual obligations.

Nadia Effendi
neffendi@blg.com

Victoria Prince
vprince@blg.com

Canadian common law in relation to GOOD FAITH performance of contracts is piecemeal, unsettled and unclear.[15]

The Trans-Pacific Partnership and the EU Agreement

In October 2015, Canada concluded negotiations with eleven other countries – including Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United States and Vietnam – on the Trans-Pacific Partnership (TPP), which is considered to be the most comprehensive trade agreement presently in existence. Taking into account the Comprehensive Economic and Trade Agreement (CETA) that Canada concluded with the European Union last year, the North American Free Trade Agreement, and a growing number of bilateral trade agreements, Canada is entering into a new era of unprecedented free trade with the United States, Mexico and many other countries throughout Central and South America, the European Union, and Pacific Asia. When these agreements are eventually ratified and implemented into Canadian law, they will affect the competitive landscape for agricultural, manufacturing and service industries throughout Canada. At the same time, they will also affect the conditions of competition for Canadian exporters of goods and services to the relevant foreign markets.

Upon coming into force, the TPP and the CETA will eliminate customs duties on almost all goods imported into Canada from the covered countries. While the elimination of some duties will apply immediately, the elimination of others will be done more gradually, so as to provide some protection while the duties are incrementally phased out over a number of years. In addition, Canadian regulation of some service sectors will be liberalized, in order to accommodate suppliers from the European Union and TPP countries.

The next stage, for both the TPP and the CETA, involves a "legal scrubbing" process to ensure that the entire text is internally consistent and coherent. Once the text of each agreement is finalized, it will be translated (in the case of the TPP, into French and Spanish; in the case of the CETA, into the official languages of each of the parties). The final stages are ratification, where each party formally accepts and enters into the agreement, and implementation, in which each party amends its domestic laws to "implement" its obligations before the date on which the agreement comes into force. There is some uncertainty about whether all of the parties, including Canada, will ratify these agreements as they presently stand. While the dates on which the TPP and the CETA will ultimately come into force are not yet known, we can expect there to be progress in the processes outlined above throughout 2016.

Now is the time when all stakeholders should be carefully investigating the potential risks and opportunities created by the TPP and the CETA with respect to specific goods and services, not only in the Canadian market but also in the relevant export markets.

Greg Tereposky
gtereposky@blg.com

The TPP currently represents a combined market of nearly 800 MILLION PEOPLE and a Gross Domestic Product (GDP) of $28.5 TRILLION.[16]

From 2012 to 2014, Canadian exports of industrial goods to TPP countries were worth, on average, $311.4 BILLION.[17]

Compliance

Market participants of every description should be increasingly concerned with regulatory compliance issues, since they affect not just the bottom line, but also one's reputation, credibility and livelihood. Further, with the election of a new federal and two new provincial governments in Canada with mandates for change, regulated conduct is likely to come under increased scrutiny, whether in the securities, insurance, trade, financial, energy or other spheres of activity. On the securities side, for example, everything from new rules to staff notices and enforcement settlement agreements warrants a closer look at one's compliance processes. In addition, declining markets have historically led to investor discontent and complaints to regulators, as well as civil actions. The cost to market participants of an investigation is high (and generally increasing), both in terms of legal costs and internal distraction. The cost of a hearing is, of course, exponentially higher on both counts, given that enforcement actions are publicly announced and have reputational consequences, regardless of the outcome (and, in addition, can provide fodder for civil actions).

The risk to public companies and others who are regulated by administrative bodies is that regulatory requirements (including a requirement to act in the nebulous "public interest") are not always clearly stated, yet require compliance in order to operate. In 2015, for example, an electricity market participant who argued that the rules were unclear was nonetheless found to have contravened market manipulation and insider trading requirements and ultimately agreed to pay over $56 million in costs and administrative penalties – a sobering reminder of the risks and uncertainties of operating in regulated markets. And also during 2015, financial industry participants were required to self-report to the securities regulators, once certain practices regarding access to lower cost investment options, available to certain qualified investors, came to light in late 2014.

The rules are becoming more and more granular, while still remaining principles-based. It is not enough to focus on the "bare bones" requirements, so executive focus (and board oversight) must be not just on daily operations and strategic initiatives but also on anticipating, planning for and responding to the objectives and policy directions of regulators, which may change depending on leadership. In light of the possible consequences and costs of regulatory investigations, significant costs are being incurred by organizations to comply with the evolving regulatory environment, its additional constraints and imposed rules. Organizations proactively establish systems to avoid complaints and scrutiny in the first instance and to respond effectively to reviews or investigations when they occur. Market participants will be acutely aware that robust compliance systems are critical to establishing "due diligence" or "reasonable investigation" defences, as well as to being able to demonstrate adherence to the "public interest", and the participants will govern themselves accordingly when carrying on business.

Rebecca Cowdery
rcowdery@blg.com

John Blair, QC
jblair@blg.com

Christian Faribault
cfaribault@blg.com

Alexander De Zordo
adezordo@blg.com

IN 2014, IT COST CANADIAN BUSINESSES
$37.1 BILLION
to comply with regulations from all levels of government.[18]

IN 2014, the TOTAL NUMBER OF HOURS spent on regulatory compliance by businesses of all sizes in Canada was

818 MILLION HOURS

which is the EQUIVALENT OF MORE THAN

419,000 FULL TIME JOBS.[19]

IN 2011, businesses with 20–99 employees spent $264 PER EMPLOYEE, or 0.18 % OF ANNUAL REVENUES, and medium-sized businesses (100 – 499 employees) spent $149 PER EMPLOYEE, or 0.18 % OF REVENUES.[20]

Canada's Anti-Spam Law – Regulatory Enforcement Begins

Canada's anti-spam law (commonly known as "CASL") creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties that prohibit unsolicited or misleading commercial electronic messages ("CEMs"), the unauthorized commercial installation and use of computer programs and other forms of online fraud.

CASL creates an opt-in regime that prohibits the sending of a CEM (subject to limited exceptions) unless the recipient has given informed consent (express or implied in limited circumstances) to receive the CEM and the CEM complies with prescribed formalities, including an effective unsubscribe mechanism. CASL applies to a regulated CEM if a computer system in Canada is used to send or access the CEM, regardless of the location of the CEM sender or CEM recipient.

In 2015, regulatory authorities began enforcing CASL against Canadian businesses, including:

(a) Compu Finder – violation notice and $1.1 million penalty for allegedly sending CEMs without consent and without a required unsubscribe mechanism;

(b) PlentyofFish Media – voluntary settlement and $48,000 penalty for allegedly sending CEMs without a required unsubscribe mechanism;

(c) Porter Airlines – voluntary settlement and $150,000 penalty for allegedly sending CEMs without proof of consent, without required information or without a required unsubscribe mechanism; and

(d) Aviscar and Budgetcar – administrative proceedings for allegedly false or misleading representations to the public, including misleading promotional emails, regarding vehicle rental prices.

The enforcement actions demonstrate that CASL violations can have potentially serious financial and reputational consequences for Canadian businesses.

Bradley Freedman
bfreedman@blg.com

Éloïse Gratton
egratton@blg.com

The CRTC has a range of enforcement tools available, from warnings to penalties (up to $1 MILLION for individuals and $10 MILLION for businesses).[21]

According to a report by Cloudmark, there was a 37% REDUCTION in spam originating from Canada (as a result of CASL). Over all, Canadians received

29% LESS EMAIL after CASL was implemented.[22]

[1] Source: *Canada's Way Forward on Climate Change*: http://www.climatechange.gc.ca/default.asp?lang=En&n=72F16A84-1

[2] Source: *Ontario Climate Change Strategy Report, 2015*: https://dr6j45jk9xcmk.cloudfront.net/documents/4914/climate-change-strategy-report.pdf

[3] Source: Government of Canada News Release: http://news.gc.ca/web/article-en.do?nid=918419

[4, 5] Source: *2015 Cost of Data Breach Study: Global Analysis* (IBM and Ponemon Institute)

[6] Source: "Class Action Intrusions: A Development In Privacy Rights or an Indeterminate Liability?" *Western Journal of Legal Studies 2015*: http://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1162&context=uwojls

[7] Source: The Global State of Information Security® Survey 2016 PWC

[8] Source: "Ashley Madison Hack Data Reveals Interesting Statistics" – *Forbes*, August 19, 2015: http://www.forbes.com/sites/tonybradley/2015/08/19/ashley-madison-hack-data-reveals-interesting-statistics/2/

[9, 10] Source: LexisNexis True Cost of Fraud 2015 Study Infographic: http://www.lexisnexis.com/risk/insights/true-cost-fraud-infographic.aspx

[11] Source: 2015 LexisNexis® Risk Solutions True Cost of Fraud℠ Study – Sept, 2015: https://www.lexisnexis.com/risk/downloads/assets/true-cost-of-fraud-2015-study.pdf

[12-14] Source: "The Future of Poison Pills in Canada: Are Takeover Bid Reforms Needed?" C.D. Howe Institute Oct. 29, 2015: https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/e-brief_219_0.pdf

[15] Source: *Bhasin v. Hrynew*, 2014 SCC 71, [2014] 3 S.C.R. 494

[16, 17] Source: Global Affairs Canada website: http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/benefits-avantages/index.aspx?lang=eng

[18, 19] Source: *Canada's Red Tape Report*: http://www.cfib-fcei.ca/cfib-documents/rr3344.pdf

[20] Source: *SME Regulatory Compliance Cost Report* – September 2013: http://www.reducingpaperburden.gc.ca/eic/site/pbri-iafp.nsf/eng/sx00149.html

[21] Source: Canada's anti-spam legislation (CASL) website: http://fightspam.gc.ca/eic/site/030.nsf/eng/home

[22] Source: *Cloudmark's 2015 Q1 Global Threat Report*: http://blog.cloudmark.com/2015/04/28/cloudmarks-2015-q1-global-threat-report/

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900, Montréal, QC H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415