



BORDEN  
LADNER  
GERVAIS

# The Year in Review: Practical Impact of Recent Developments

**Julio Arboleda & Robert J.C. Deane**

Special thanks to Cherie Mah, Student – at - law



# Introduction

- **This presentation will be a high level review of selected recent fundamental developments in privacy and related law.**
- **Concentration on Alberta, British Columbia and Federal jurisdictions, as well as selected international developments.**
- **This presentation does not consider health information developments.**



BORDEN  
LADNER  
GERVAIS

# *Disclaimer*

**This presentation is not intended to provide legal advice. We urge you to consult your legal counsel if you have any questions relating to the needs of your organization.**



# Agenda

1. **Statutory Reviews of Privacy Legislation – What Happened to the Momentum?**
2. **Cross-Border Flow of Consumer Information**
3. **Exploring the Limits of Privacy Commissioners’ Jurisdiction**
  - (A) Jurisdiction – Abika and LSAC
  - (B) Facebook and Social Networking Sites
  - (C) Regulating the Private Sector – Personal Information on the Web
4. **Introducing A New Era of Private Sector Regulation?**
  - (A) Identification Document Collection
  - (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private Sector Regulation
  - (C) Significant Developments Outside of PIPA-PIPEDA Framework – Private-Sector Regulation of the Internet
5. **Collection and Distribution of Employee Information**



# Statutory Reviews of Privacy Legislation – What Happened to the Momentum?

- **British Columbia *Personal Information Protection Act* (PIPA)**
  - ◆ First report came out April 2008
  - ◆ Uncertain when recommendations will be tabled and when Act will be amended
  - ◆ Third statutory review committee struck in October 2009
- **Alberta *Personal Information Protection Act* (PIPA)**
  - ◆ First report came out November 2007
  - ◆ Motion for a Bill to amend PIPA will likely be made in February 2010



# Statutory Reviews of Privacy Legislation – What Happened to the Momentum?

- **Canada *Personal Information Protection and Electronic Documents Act* (PIPEDA)**
  - ◆ First report in May 2007; reviewed and responded to by Industry Canada; further consultations required
  - ◆ Waiting for special proposals for legislative and non-legislative action
- **Quebec *Commission d'accès à l'information* (AAPI)**
  - ◆ Recommendations made at 2009 annual convention may be taken into consideration for the 2011 scheduled review of the Act



# Cross-Border Flow of Consumer Information

- ***Datatreasury Corp. v. Royal Bank of Canada* [2008] F.C.J. No. 1193**
  - At issue was sending sensitive litigation information to the US
  - Court disallowed draft Canada Only Clause restricting Canadian customers' confidential info from being sent across borders
  - PIPEDA applies - but personal Information not really at issue, and no good evidence of actual risk to Bank Group litigants
  - Final protective Court Order helpful in foreign country, detailing maintenance of confidential aspects of patented technology; confidential pricing and cost information and confidential business practices re: terms/conditions of licensing and settlement agreements



# Cross-Border Flow of Consumer Information

## ■ **PIPEDA Case Summary #2008-394, (Sept. 2008)**

- Outsourcing of canada.com email services to U.S.-based firm raised questions for subscribers e.g. PATRIOT Act
- PIPEDA permits international outsourcing
- Organizations to assess security risk to customer personal information upon transfer to foreign-based service provider
- Transparency and notice of cross border collection and use of customer personal information required
- “Essential” that organizations using foreign service providers use contractual or other means to provide a comparable level of protection
- **Helpful Resource:** The Federal Privacy Commissioner’s *Guidelines for Processing Personal Data Across Borders*  
[http://www.priv.gc.ca/information/guide/2009/gl\\_dab\\_090127\\_e.pdf](http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf)



# Exploring the Limits of Privacy Commissioners' Jurisdiction

**(A) Jurisdiction – Abika & LSAC**

**(B) Facebook and Social Networking Sites**

**(C) Regulating the Private Sector – Personal Information on the Web**



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (A) Jurisdiction

- ***Canada (Privacy Commissioner) v. Blood Tribe Department of Health, [2008] S.C.J. No. 45***
  - ◆ Former employee requested employment documents
  - ◆ Complained after employer withheld solicitor-client privileged documents from records provided
  - ◆ Privacy Commissioner's order for production of privileged documents overruled by the Federal Court of Appeal. Court's decision upheld by the Supreme Court of Canada



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (A) Jurisdiction

- ***Canada (Privacy Commissioner) v. Blood Tribe Department of Health, [2008] S.C.J. No. 45***
  - ◆ Privacy Commissioner did not have the power to order the production of solicitor-client privileged documents
  - ◆ Privacy Commissioner may forward information to Attorney General and may even become adverse in interest to person claiming privilege
  - ◆ Compelled disclosure to an administrative officer would constitute an infringement of the confidentiality of the solicitor-client communications
  - ◆ **Note: this is different from the BC and Alberta Privacy Commissioners who have additional powers and have developed separate processes for reviewing privilege claims**



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (A) Jurisdiction

- ***Lawson v. Accusearch* [2007] 4 F.C.R. (“Abika”) and *Abika Report of Findings, (July 2009)* and *Law School Admission Council Investigation (“LSAC”) (May 2008)***
  - ◆ In Abika Federal Court said Privacy Commissioner has jurisdiction to investigate the trans-border flow of personal information of Canadians - Basis for jurisdiction is “in materium”
  - ◆ In LSAC Privacy Commissioner relied on “real and substantial connection”
  - ◆ Significant decisions as U.S. and overseas businesses and their Canadian operations can expect Canadian privacy laws enforced even across borders
  - ◆ Subsequent Abika shows significant investigative cooperation between Privacy Commissioner and U.S. Federal Trade Commission



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (A) Jurisdiction

### ■ Query:

- Can similar jurisdictional arguments (real and substantial connection and jurisdiction in materium) be applied to the Provincial Privacy Commissioners?
- What would happen in the absence of cooperation among the Federal/Provincial Commissioners?
- What about different Federal Provincial jurisdiction over employee information?



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (B) Facebook and Other Social Networking Sites

- Facebook *PIPEDA Case Summary #2009-08, (July 2009)* and follow up *Reporting Letter, (Aug. 2009)*
  - ◆ Case Summary 100 pages!
  - ◆ 12 Million Canadian users, 100's of thousands of third party application developers in 180 countries
  - ◆ Central issues in complaint were knowledge and consent, retention and security safeguards
  - ◆ Facebook agreed to make significant privacy changes including disclosure, collection, default privacy settings, account deletion options and third party applications



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (B) Facebook and Other Social Networking Sites

- **Assistant Federal Privacy Commissioner on Facebook:**
  - ◆ “Our Office has made clear our expectations for how social networking sites need to protect personal information. Other sites should take note – and take steps to ensure they’re complying with Canadian law.”
- The word “jurisdiction” does not appear in case summary – just asserted that PIPEDA applies
- Cutting edge regulatory approach with practical impact anywhere in the world



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (B) Facebook and Other Social Networking Sites

### ■ **Federal Privacy Commissioner's Comparative Report of 6 Social Networking Sites (SNS) (Feb 2009)**

- ◆ Analyzed privacy-specific characteristics
- ◆ Concluded privacy issues arise from a gap between users' contextual understanding and actual scope of information flow
- ◆ Advised SNS' provide meaningful privacy controls, protections and to identify/understand user expectations



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (C) Regulating the Private Sector – Personal Information on the Web (Canada)

- *PIPEDA Case Summary #2009-010, (Sept. 2009)*
  - ◆ Complaint that Bell Sympatico uses Deep Packet Inspection (DPI) to collect information from customers without consent, more than necessary to ensure service, and that proper notice of this is not given
  - ◆ DPI usually used with traditional firewall technology – now used by Bell and other ISPs in traffic management
  - ◆ Allows for examination of not only application and subscriber usage patterns etc. but also the payload content of user communication (user's emails, pictures and information)
  - ◆ Complaint not well founded on consent and limiting collection, but Privacy Commissioner recommended Bell clarify and explain to customers its practices and DPI's privacy impact



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## (C) Regulating the Private Sector – Personal Information on the Web (United States)

- US Federal Trade Commission's desire to limit practice of delivering ads to individuals based on Web pages visited and searches carried out
- FTC Chairman:
  - ◆ “There’s a critical issue about whether consumers have notice of what companies are doing with their information and whether they’re making informed choices about [sharing] information.”



# Exploring the Limits of Privacy Commissioners' Jurisdiction

## *Cont'd...*

- Regulation has implications for companies that depend on Web advertising and engage in some form of targeting (e.g. Google, Facebook, Microsoft)
- Industry self regulation not “moving far enough or fast enough” – FTC Chairman
- Congress readies opt-in consent bill
  - ◆ Attempt to have more internet targeted-ads require opt - in consent from web users before collecting data



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

- British Columbia, Alberta, Federal Decisions

## (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private-Sector Regulation

- Bill C-46, *Investigative Powers for the 21<sup>st</sup> Century Act* (IP21C)
- Bill C-47, *Technical Assistance for Law Enforcement*

## (C) Significant Developments Outside of PIPA-PIPEDA Framework – Private-Sector Regulation on the Internet

- Bill C-27, *Electronic Commerce Protection Act* (EPCA)
- France – “3 Strikes, You’re Out”



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

### ■ **British Columbia – Ensuring Public Safety**

- ◆ Cruz Ventures Ltd., Order P09-01 (July 21, 2009)
- ◆ Patron complained about bar which swipes drivers licenses and takes digital photographs
- ◆ Patrons who disagreed with collection disallowed entry
- ◆ System recorded date/time each customer entered premises and tracked number of visits
- ◆ At time of complaint, records retained for six months and would be “reset” if customer visited within the six months
- ◆ “Incidents” reports recorded for up to a year, but if a second incident occurred and recorded, original report visible until expiry of second report.
- ◆ Software set up to allow other establishments to access information about incidents/alerts



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

### ■ **British Columbia – Ensuring Public Safety**

- ◆ OIPC concluded that purposes were valid – directly related to the supply of the product or service (improve safety and prevent minors from access); but evidence did not establish that the collection and storage was integral to purpose
  - Acceptable to collect some personal information, but collection of license numbers and extended retention not shown to be necessary or appropriate
- ◆ Mandatory consent also an issue – OIPC did not accept that consent could be deemed as being obvious to a reasonable person
- ◆ OIPC found that inadequate notice of collection and purposes had been given



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

### ■ **British Columbia – Ensuring Public Safety**

- ◆ New software, EnterSafe, only collects: name, photograph, birth date and gender; information held for no more 24-hours unless customer is violent or otherwise undesirable from safety perspective
- ◆ If incident occurs in 24-hour period, information could be kept and shared with other bars using this software
- ◆ **Example of an industry responding to an arguably case-specific decision: Privacy Commissioner leveraging adjudicative and consultative functions**



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

- **Alberta – No Connection Established Between Collection and Patron Safety but Legislation Will Likely Change This**
  - ◆ *Penny Lane Entertainment Ltd., Tantra Night Club Inc.* Order P2006-011 (February 15, 2008)
  - ◆ Organization argued scanning system was for patron safety and to discourage would-be trouble-makers from entering venue
  - ◆ **Privacy Commissioner found:**
    - On the evidence, no reasonable purpose (per s. 11 of PIPA) for collecting and retaining patron driver’s license information



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

### ◆ Privacy Commissioner found:

- No correlation between violence, patron safety and collection and retention of information
- Lack of evidence to show that scanning drivers’ licenses would make the bar safer, encourage patrons to behave, or reduce violence

- ◆ *Penny Lane Entertainment Group v. Alberta (Information and Privacy Commissioner)*, [2009] A.J. No. 300 upheld Privacy Commissioner’s decision



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

- **Bill-42, *Gaming and Liquor Amendment Act, S.A. 2009 c. 23***
  - ◆ Received Royal Assent June 4, 2009
  - ◆ Effectively reverses Privacy Commissioner’s decision
  - ◆ Allows collection of person’s name, age, photograph and if licensee knows or reasonably believes person engaged in unlawful activities, can disclose information to other licensees
  - ◆ *Must also be disclosed to police on request*



# Introducing A New Era of Private-Sector Regulation?

## (A) Identification Document Collection, “BarWatch”

### ■ Federal – Unresolved Contention

- ◆ *PIPEDA Case Summary #2008-396, (May 2009)*
- ◆ Patron entered licensed Canad Inns – driver’s license copied by an ID machine and patron was recorded on video surveillance
- ◆ Establishment followed recommendations to modify signage, limit surveillance retention, but refused to cease using ID machines and to remove information already collected
- ◆ Privacy Commissioner filed an application before Federal Court



# Introducing A New Era of Private-Sector Regulation?

## (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private-Sector Regulation

- **Bill C-46, *Investigative Powers for the 21<sup>st</sup> Century Act (IP21C)***
  - ◆ **Authority to order telecommunications providers and others to preserve and turn over data regarding subscribers – for example:**
    - Judicial warrant to trace mobile devices and their owners and compel disclosure of tracking information
    - Demand a service-provider maintain certain data until warrant or production order is obtained if reasonable grounds to suspect offence has or will be committed
    - Allow police to request a service-provider to preserve data or provide a document even without a preservation order or legally-sanctioned mechanism
  - ◆ **Liability shield for a person who engages in such cooperative activity with police**



# Introducing A New Era of Private-Sector Regulation?

## (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private-Sector Regulation

- **Bill C-47, *Technical Assistance for Law Enforcement***
  - ◆ Impacts wireless service providers, internet access providers, most VOIP providers
  - ◆ Potentially broad enough to include non-access providers like e-mail application providers, web hosting facilities
  - ◆ Key requirement is that service-providers be able to intercept communications traffic and permit access to authorized officials
  - ◆ Non-designated officers also have access in urgent situations



# Introducing A New Era of Private-Sector Regulation?

## (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private-Sector Regulation

- **Do Bill C-46 and C-47 Practically Change the *Status Quo*?**
  - ◆ ***R. v. Wilson*, [2009] O.J. No. 1067:** Court ruled IP address not particularly sensitive and customer had no reasonable expectation of privacy as he had signed Bell Canada's Privacy Policy
  - ◆ ***R. v. Vasic*, [2009] O.J. No. 685:** Combining customer name and address info with IP address data could be sensitive but upheld disclosure without warrant since customer consented to Rogers' Acceptable Use Policy
  - ◆ Production Orders under the *Criminal Code*



# Introducing A New Era of Private-Sector Regulation?

## (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private-Sector Regulation

### ■ Implications of Bills C-46 and C-47

- ◆ Privacy concerns
- ◆ Law enforcement powers not limited to serious criminal offences but could be used to target minor, non-criminal matters – “purpose creep”
- ◆ “Protecting Privacy for Canadians in the 21<sup>st</sup> Century: Resolution of Canada’s Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47” (September 9-10, 2009):  
“Canadians put a high value on the privacy, confidentiality and security of their personal communications and our courts have also accorded a high expectation of privacy to such communications. The current proposal will give police authorities unprecedented access to Canadians’ personal information.”



# Introducing A New Era of Private-Sector Regulation?

- (B) Significant Developments Outside of PIPA-PIPEDA Framework – Government-Imposed Private-Sector Regulation
  - **Bills C-46 and C-47 Similar to European Data Retention Directive (April 2009)**
    - ◆ Details of user emails and net phone calls stored by ISPs accessible by authorities without a warrant



# Introducing A New Era of Private-Sector Regulation?

## (C) Significant Developments Outside of PIPA-PIPEDA Framework – Private-Sector Regulation on the Internet

### ■ **Canada’s Bill C-27, *Electronic Commerce Protection Act (EPCA)***

- ◆ Regulatory scheme to deal with spam
- ◆ Privacy Commissioner specifically empowered to refer complaints to CRTC and Competition Bureau
- ◆ PIPEDA amended to allow Privacy Commissioner to share information with all provincial counterparts and foreign counterparts enforcing similar laws – applies to all activities, not just spam
- ◆ Prohibits collection of personal information by unauthorized access

### ■ **France’s “3 Strikes, You’re Out” Policy**

- ◆ New state agency – the High Authority of Diffusion of the Art Works and Protection of Rights on the Internet (“Hadopi”)
- ◆ First sends illegal file-sharers a warning email, a letter, and then finally cuts off connection (subject to Hadopi obtaining written order from a judge)
- ◆ Internet users with a Wi-Fi connection must block unauthorized users from accessing



# Introducing A New Era of Private-Sector Regulation?

## ■ Query:

- Are these developments indicative of a new layer of technology or type-specific private-sector regulation?
- Is the information that is the regulated subject matter being regulated because it is now recognized to be a major economic force?



# Collection & Distribution of Employee Information

## ■ *Sochowski v. British Columbia (IPC)*, 2008 BCSC 130

- Employee complained about company's requirement that employees provide drivers' abstracts
- Employee did not have standing because policy did not apply to him as company made accommodations to only request his driver's license, not insurance abstract – complaint unwarranted
- Entitling “any employee to complain about anything that an employer does or fails to do even if it has no direct effect upon [them]...would entitle the ‘mere busybody’ involvement that was said to be insufficient even on public policy grounds”
- Detailed consideration of commissioner's functions (adjudicative/inquisitorial/educative)



# Employer Collection & Distribution of Employee Information

## ■ *Johnson v. Bell Canada*, [2008] F.C.J. No. 1368

- Employee complained Bell carried out inadequate search after he requested access to emails concerning him in the company from all sources
- Submitted Bell breached PIPEDA when they deleted relevant personal emails
- Personal emails did not have to be produced because they did not have a business purpose
- Highlights differences between PIPA and PIPEDA, and undermines historical notion of the workplace as a “privacy-free” zone



# Employer Collection & Distribution of Employee Information

- ***Empire Ballroom (1208558 Alberta Ltd.), P2008-IR-005***
  - Employee complained about having to use thumbprint sign-in system at start of shifts
  - Thumbprint sign-in system for employees translated prints into “unique numeric identifiers”
  - Remained personal information, but was collected for a reasonable purpose
  - However, employer failed to explain what personal information was being collected, and failed to provide its privacy policy
    - ◆ Allegation: “*You work for me, I am your privacy policy*”



# Employer Collection & Distribution of Employee Information

- ***Pietrylo v. Hillstone Restaurant Group*, Docket No. 2:06-cv-05754 (D.N.J. 2008) (USA)**
  - Plaintiffs created MySpace user group for current and former employees to vent about working at the restaurant
  - Plaintiffs terminated when employer discovered group
  - Reasons: violation of company policy involving “professionalism and a positive attitude”
  - No expectation of *privacy* in social media though employer’s act a violation of US law
  - Same or different approach in Canada?



BORDEN  
LADNER  
GERVAIS

# Thank You!

**Julio Arboleda**

[JArboleda@blgcanada.com](mailto:JArboleda@blgcanada.com)

**403-232-9601**

**Robert J.C. Deane**

[RDeane@blgcanada.com](mailto:RDeane@blgcanada.com)

**604-640-4250**