Hot Topics in Privacy and Cybersecurity Law

BCHIMPS
Annual Spring Educational Symposium
Vancouver, March 2, 2018

Bradley J. Freedman
bfreedman@blg.com

Borden Ladner Gervais

Agenda

- Introduction/Background and Legal Framework
- Data Minimization and De-identification
- Data Security Breach Obligations
- Contracting with Data Processors/Service Providers
- Legal Compliance and Risk Management

Borden Ladner Gervais

Key Concepts

Personal Information – information about an identifiable individual, including information that can be used with other information to identify an individual.

Cyber risk – risk of harm or liability resulting from damage/disruption to information technology systems (internal or external) or a data security incident.

Data security incident – unauthorized access, use, disclosure, modification or deletion of regulated, protected or sensitive data.

Cybersecurity – physical, organizational and technological measures (people, practices and processes) designed to manage cyber risks.

Borden Ladner Gervais

Privacy – A Fundamental Human Right

"The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy." Alberta v. United Food and Commercial Workers, SCC

"… privacy is at the heart of liberty in a modern state; … privacy is essential for the well-being of the individual". R. v. Dyment, SCC

… privacy is "a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society". R. v. Spencer, SCC

BLG
Borden Ladner Gervais

Privacy – Medical Ethics

Canadian Medical Association Code of Ethics

"Take all reasonable steps to prevent harm to patients; should harm occur, disclose it to the patient."

"Protect the personal health information of your patients."

"Be aware of your patient's rights with respect to the collection, use, disclosure and access to their personal health information …"

"Disclose your patients' personal health information to third parties only with their consent, or as provided for by law …"

Borden Ladner Gervais

Cyber Incident Harm to Individuals

- humiliation, psychological harm
- damage to reputation or relationships, discrimination, stigmatization
- loss of employment, business or professional opportunities
- financial loss / economic harm
- identity theft
- negative effects on credit record
- loss of trust/confidence in health care system

Borden Ladner Gervais

Cyber Incident Harm to Organizations

- business disruption
- alteration/loss of data
- disclosure of sensitive data
- remediation costs
- costs of regulatory investigations/proceedings and civil litigation
- liability to affected individuals (patients/employees) and organizations
- regulatory fines and other sanctions/discipline

Borden Ladner Gervais

Health Industry – High Risk Profile

- PHI - extremely sensitive and high criminal value
- Distributed, patchwork, rapidly changing IT infrastructure
  - personal mobile data devices, smart/connected medical devices, legacy systems, cloud services, EMR, EHR, AI
- Personnel challenges
- Financial challenges
- External and internal sources of risk/liability
  - cyber criminals, conventional criminals: ransomware, data exfiltration, physical theft
  - workers and service providers: cyber and conventional errors and intentional misconduct (and vicarious liability)

Borden Ladner Gervais

Legal Framework

Organizations in BC

- *Personal Information Protection Act* (PIPA) – privacy sector
- *Freedom of Information and Protection of Privacy Act (FIPPA)* – public sector
- Common law / civil law duties and sector specific laws

Organizations in Other Provinces

- Provincial personal information / health information protection statutes
- Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)
- Common law / civil law duties and sector specific laws

Globalization (Raising the Bar)

- European Union *General Data Protection Regulation*

BLG
Borden Ladner Gervais

Data Minimization and De-identification

Data Minimization Principle

- Collect and disclose the minimum amount of data required for a legitimate purpose, retain data only as long as required for the legitimate purpose and legal compliance, securely destroy/de-identify data when no longer needed
- A fundamental principle of Canadian personal information protection statutes

De-Identification

- Can be an effective way to comply with Data Minimization Principle
- Anonymization and pseudonymization

Borden Ladner Gervais

Data Minimization and De-identification

- Privacy Commissioner recent decisions (*Ashley Madison* - 2017) and guidance emphasize importance of Data Minimization Principle
- Increasing awareness/emphasis as a result of European Union GDPR
- Key consideration for Big Data programs, data sharing and research
  - BC Privacy Commissioner *Access to Data for Heath Research* (January 2018)
- Important cyber risk management tool

Borden Ladner Gervais

Data Security Breach Obligations

BC PIPA and FIPPA – current state

- No express statutory obligation to report breaches to Privacy Commissioner or notify affected individuals
- Reporting and notification of certain breaches is required for public sector organizations, and encouraged for privacy sector organizations

PIPEDA – current state

- No express statutory obligation to report breaches to Privacy Commissioner or notify affected individuals
- Breach reporting to Privacy Commissioner is encouraged

Borden Ladner Gervais

Data Security Breach Obligations

PIPEDA – amendments soon in force

- Maintain prescribed records of every “breach of security safeguards”, and disclose records to Privacy Commissioner on request
- If a breach presents a “real risk of significant harm” to individual:
  - deliver prescribed report of breach to Privacy Commissioner
  - give prescribed notice by prescribed method to all individuals
  - give notice of breach to other organizations/government institutions
- Knowing contravention – up to $100,000 fine
- Possible further requirements to maintain GDPR equivalence

Borden Ladner Gervais

Data Security Breach Obligations

Provincial Laws – predicted future amendments

- Record keeping and reporting obligations substantially similar to PIPEDA or more stringent GDPR, to maintain substantial similarity or equivalence

Existing Common Law / Civil Law and Ethical Obligation

- Give notice of breach to help affected individuals and organizations avoid or mitigate harm
- Required by general common law/civil law duty of care
- Pragmatic considerations

Borden Ladner Gervais

Data Processors/Service Providers

Statutory Duties on Personal Information Controllers

- **Accountability:** Organizations that collect personal information are accountable for the information, including information transferred to other organizations for processing or storage
- **Protection/Safeguards:** Organizations that collect personal information must "protect' or "safeguard" the personal information using "reasonable security arrangements" or "security safeguards" appropriate to the sensitivity of the information" and contractual measures
- **Location:** BC public bodies must store and access personal information only in Canada

Old School Duties: Duties of care and governance duties

Industries/Sectors: Specific requirements and best practices guidance

BLG
Borden Ladner Gervais

Data Processors/Service Providers

Practical challenges to legal compliance

- Most statutory obligations focus on personal information/data controllers
- Data controllers cannot outsource legal compliance obligations
- Data controllers often have limited negotiating leverage with service providers

Potential Changes to Anticipate

- Amendments to Canadian statutes – for GDPR equivalency
- Possible new BC PHI statute like some other provinces, recommended by Privacy Commissioner
- Changing attitudes by some processors

Borden Ladner Gervais

Legal Compliance / Risk Management

Regulatory guidance for health care sector

- Privacy Commissioners
  - *BC Physician Privacy Toolkit* (Aug. 2017)
  - *Exam of BC Health Authority Privacy Breach Mgmt.* (Sept. 2015)
  - Ontario Privacy Commissioner - cloud computing and de-identification
  - “Accountability” and ”Safeguards” guidance
  - Previous decisions

Best practices from other industries/sectors and other countries

- Critical infrastructure and financial services
- UK and EU *GDPR* guidance

Borden Ladner Gervais

Legal Compliance / Risk Management

People, Practices and Processes | Physical, Organizational and Technological

- An enterprise risk issue; not simply an IT issue
- Documented, best practices framework with C-suite oversight
- Periodic assessments of risks and controls
- Awareness education and training
- Policies and procedures
- Technology tools – properly implemented and effectively used
- Incident preparation – IRP and TTX
- A continuous process – the new normal

Insurance

- Rapidly changing market
- Consider (periodically) insurance coverage for residual risk

BLG
Borden Ladner Gervais

Questions

Borden Ladner Gervais

Thank You

Borden Ladner Gervais