

DATA BREACHES: What You Need to Know

CLARK WILSON 


Presented by:
 Scott Lamb, Partner, Clark Wilson LLP
 Jeff Holowaychuk, Partner, Clark Wilson LLP
 Mark Rowan, Chief Executive Officer, Data Sentinel

(September 21, 2023) CW20077292

1

Lifecycle of a Privacy Breach


1. Overview of Legal Obligations
2. Actions Following Privacy Breach
3. Notification Obligations
4. Preventative Measures

CLARK WILSON  2

2

Overview of
Legal Obligations

Scott Lamb, Partner, Clark Wilson LLP
 604 643 3103 | slamb@cwilson.com

CLARK WILSON  3

3

What is Privacy Law in Canada?

- Broad range of concepts, legislation and case law
- Rapidly evolving and growing body of law

CLARK WILSON DATA SENTINEL 4

4

Federal Privacy Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Private sector regulation of personal information (January 1, 2004)
- Federally regulated industries (banks, telecoms, airlines)
- Inter-provincial and international exchange of personal information
- Provinces who have failed to pass their own similar privacy law.

Privacy Act

- Public sector regulation of personal information (1983)
- Covers approximately 260 Federal government institutions

CLARK WILSON DATA SENTINEL 5

5

Provincial Privacy Legislation

British Columbia
Alberta
Quebec

Healthcare Sector:
Saskatchewan
Manitoba
Ontario
New Brunswick
Nova Scotia
Newfoundland and Labrador

CLARK WILSON DATA SENTINEL 6

6


BC Privacy Legislation

Personal Information Protection Privacy Act (PIPA)

- January 2004 implemented
- Private sector regulation of personal information within British Columbia

Freedom of Information and Protection of Privacy Act (FIPPA)


- November 2021 amended
- Public sector regulation of personal information within British Columbia

CLARK WILSON  7

7

Ten Principles


- 1. Accountability**
 - An organization shall designate an individual to be accountable for compliance.
- 2. Identity Purposes**
 - The purposes for which personal information is collected shall be identified.
- 3. Consent**
 - The knowledge and consent of the individual are required except where appropriate.

CLARK WILSON  8

8

Ten Principles

- 4. Limiting Collection**
 - The collection of personal information shall be limited to that which is necessary for purposes identified.
- 5. Limiting Use, Disclosure and Retention**
 - Personal information shall not be used or disclosed for purposes other than those for which it was collected.
 - Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

CLARK WILSON  9

9

Ten Principles

6. Accuracy
 – Personal information shall be accurate, complete and up-to-date.

7. Safeguards
 – Safeguards shall be used appropriate to the sensitivity of the information.

8. Openness
 – An organization shall make readily available to individuals specific information about its policies and practices.

CLARK WILSON DATA SENTINEL 10

10

Ten Principles

9. Individual Access
 – An individual shall be informed of the existence, use and disclosure of their personal information.
 – The individual shall be given access to the information and be able to challenge the accuracy and completeness of it and have it amended as appropriate.

10. Challenging Compliance
 – An individual shall be able to address a challenge concerning compliance to the designated individual responsible for compliance in the organization.

CLARK WILSON DATA SENTINEL 11

11

What's New in Privacy Law

- **Reform of Federal Law**
 - Bill C-27 to replace PIPEDA with new Consumer Privacy Protection Act (CPPA)
 - Same framework as PIPEDA
 - Modernize in line with international standards (EU-GDPR and California – CCPA)
 - Implement new law 2023?
- **Reform of BC Law**
 - FIPPA (Public Sector)
 - o November 2021 – Royal Asset
 - o February 2023 – Mandatory Breach Notification
 - PIPA (Private Sector)
 - o Special Committee of BC Legislature – 34 recommendations
 - o Modernize in line with Federal and international standards;
 - o Introduce proposal amendments in 2023?


CLARK WILSON DATA SENTINEL 12

12

Significant Changes in CPPA

Enforcement

- Privacy Commissioner given enhanced powers
- Privacy Commissioner conducts inquiry after investigating compliant or non-compliance with agreement
- Privacy Commissioner renders decision – if contravention of CPPA – fail to report data breach:
 - Issue a compliance order
 - Recommend Tribunal impose penalty


CLARK WILSON  13

13

Significant Changes in CPPA

Enforcement (cont'd)

- Tribunal has power to impose penalty of up to \$10 million or 3% of gross revenue, whichever is higher
- Tribunal can also award penalty of up to \$25 million or 5% of gross revenue where organization:
 - knowingly contravened breach reporting and notification
 - knowingly contravened requirements to retain personal information that is subject to access request
 - knowingly used de-identification information to identify an individual
 - knowingly contravened a compliance order
 - obstructed Privacy Commissioner in an investigation, inquiry or audit.


CLARK WILSON  14

14

Significant Changes in CPPA

Private Right of Action



- Where Privacy Commissioner finds a contravention of CPPA
- Class Actions for data breaches

CLARK WILSON  15

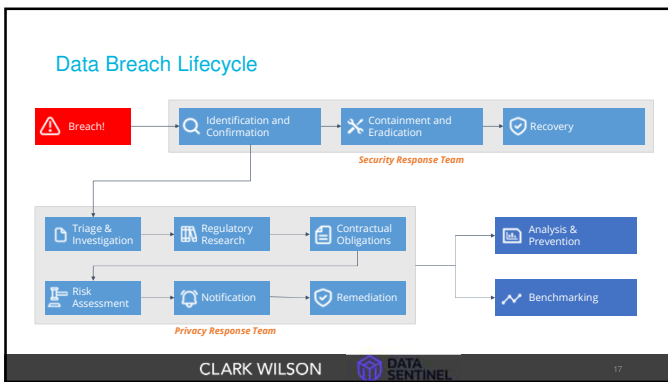
15

Actions Following a Privacy Breach

Mark Rowan, CEO, Data Sentinel
416-570-6228 | mark@data-sentinel.com

16



17

Detection and Action

Assemble a Response Team:
This team might include IT professionals, cybersecurity experts, legal counsel, PR and communications specialists, and relevant management personnel. If you don't have sufficient expertise in-house, you might need to hire external specialists.

Engage a Forensic Investigation:
A thorough forensic investigation will help you understand what happened, how it happened, and how the attacker accessed your network. This involves analyzing system logs, understanding patterns of behaviour, and identifying the exploited vulnerabilities.

Assess the Scope of the Breach:
Understand what data was accessed or stolen. This might involve a detailed data investigation. Knowing the type of data that was compromised, the affected individuals, and other sensitive data is a critical step in preparation for disclosure.

Identify the Source of the Breach:
Use forensic evidence to identify the source of the breach. This could involve malware analysis, studying network logs, or analyzing any unusual activity.

Cooperate with Regulators, Law Enforcement:
In cases where criminal activity is suspected, you will likely need to work with local or national law enforcement agencies. They can also help to investigate the breach and possibly identify the culprit.

In the Next Section - Containment and Prevention

Fix the Vulnerabilities:
Once you know how the breach occurred, fix the identified vulnerabilities. This might involve patching software, tightening network security measures, or improving access controls.

Improve Security Infrastructure:
Depending on the nature of the breach, it may be necessary to invest in new security tools and technologies. This could involve better network monitoring tools, intrusion detection systems, or advanced encryption technologies.

Enhance Access Controls and Policies:
Review your policies and controls related to data access. Implement stricter controls if necessary. This could include stronger password requirements, two-factor authentication, and limiting access to sensitive data.

Train Employees:
If the breach was caused by human error, it's important to provide additional training to your staff. Make sure they understand the latest threats and their role in maintaining the security of the organization.

Conduct Regular Audits and Penetration Testing:
Regular audits of your IT systems can help identify any remaining vulnerabilities or compliance issues. Penetration testing can help identify weaknesses in your security posture.

Establish a Disaster Recovery Plan:
If you don't already have a disaster recovery plan, now is the time to establish one. This plan will provide a roadmap for recovering from future security incidents and minimizing downtime.

These steps should be tailored to the specifics of the breach and your organization. The goal is to understand the breach fully and take measures to prevent similar incidents in the future.




18

Data Discovery Requirements


Jeff will speak to this in detail.

- Details of the Sensitive Data:
 - Types of data compromised (e.g., PII, PCI, PHI, Corp IP, etc.)
 - Number of individuals affected
 - Geographical location of the affected individuals
 - Details of each individual affected
- Impact Analysis:
 - Impact on individuals (e.g., potential for identity theft, financial loss)
 - Impact on the organization (e.g., financial, reputation)

CLARK WILSON DATA SENTINEL 19

19

What is Automated Data Discovery



Technology and processes used to collect, classify and analyze data from various sources to gain insights rapidly, accurately and cost effectively.

CLARK WILSON DATA SENTINEL 20

20

Automated Data Discovery Process

Data Discovery Breach Response Activities						
Breach Notification	Initiation	Planning & Environment Configuration	Data Discovery & Classification Initiation	Continue Discovery & Classification Process	Analysis, Refinement, Breach Support Efforts	Breach Response Deliverables
<ul style="list-style-type: none"> ✓ Requirements defined ✓ Key Stakeholders engaged ✓ Kick-off 	<ul style="list-style-type: none"> ✓ Technical workshop with IT and Security, Initiate and connect. ✓ Data Classification & Policy overview. ✓ Data classification and policy mapping define custom class requirements. ✓ Configure and test connectivity. 	<ul style="list-style-type: none"> ✓ Run automated classification discovery process sample. ✓ Review of initial source results. Capture any adjustments to classifications or policy mapping. ✓ Apply classification updates, Custom or exclusions ✓ Initiate discovery & classification on all data. ✓ Do interim reviews. 	<ul style="list-style-type: none"> ✓ Review discovery & classification results by high/low source groupings. ✓ Provide access to initial detailed reports/ views. ✓ Align breach reporting requirements with the results. 	<ul style="list-style-type: none"> ✓ Review of output and Analysis. ✓ Adjust and rerun data classification process based on analysis results (Exclusions, custom classifications or views), if Applicable. ✓ Finalize and produce complete inventory of sensitive data (PI, PCI, PHI and any custom classes). ✓ Finalize the affected data subject report. ✓ Prepare summary reports and extract files. 	<ul style="list-style-type: none"> ✓ Present detailed findings. ✓ Present disclosure report ✓ Establish next steps, if any. 	

CLARK WILSON DATA SENTINEL 21

21

Report Generation

Common Output Request Examples:

- Sorted list of high-risk files
- All files containing specific PII
- All Unique SIN or SSN found
- PCI or PHI Information
- All Unique E-Emails found
- All Unique Person Names found
- Lists of statutory documents
- Files containing specific targets
- Identity 360

Field Name	Description of Content	Example Value
Source	Server where classification was completed	Data Sentinel Server 1
Vendor	Source of data	File Servers
File Server	Name of file server where object was found	(File Server)
Object Location	Location of the file (complete)	/(key location)/LETTERS
Object Name	Name of the file	Vendor Account (##).PDF
Classification Family	Group of Classifications	Social, Technology, Finance
Classification Sensitivity	Sensitivity Group	PCI, PII, PHI
Classification Summary	Classification names associated with file	Email, phone
Classification w/ Data	Classification name plus related datapoint(s)	Payroll(T4); payment(void cheque)

22

22

Notification Obligations

Jeff Holowaychuk, Partner, Clark Wilson LLP
 804 643 3194 | jholowaychuk@cwilson.com

23

23

Mandatory Breach Notification

Timeline of Mandatory Breach Notification Requirements in Canadian Jurisdictions

- Alberta PIPA (privacy sector) – May 1, 2010
- Federal PIPEDA (private sector) – November 1, 2018
- Quebec Law 25 (private sector) – September 22, 2022
- BC FIPPA (government and public bodies) – February 1, 2023
- BC PIPA (private sector) – ???


24

24

Mandatory Breach Notification

What is a “privacy breach”?

- Theft or loss, or unauthorized access to, collection, use or disclosure of personal information in the custody or under the control of an organization.
- Examples:
 - Send personal information to wrong email recipient
 - Lost laptop, USB stick or other device containing personal information
 - Ransomware / hacking


CLARK WILSON  25

25

Mandatory Breach Notification

When must an organization make notification?

- Notification to the Privacy Commissioner and affected individuals must be made where it is reasonable to believe there will be a **“real risk of significant harm to the individual”**:
- This includes:
 - identity theft,
 - bodily harm,
 - humiliation,
 - damage to reputation or relationships,
 - loss of employment, business or professional opportunities,
 - financial loss,
 - negative impact on credit record, or
 - damages to, or loss of, property.
- Notification must be made without unreasonable delay.


CLARK WILSON  26

26

Mandatory Breach Notification

FIPPA and RROSH

- Oddly, the language in FIPPA for triggering notification obligation depends on **“if the privacy breach could reasonably be expected to result in significant harm”**, which differs from the Federal PIPEDA and Alberta PIPA legislation where notification is required where there is a **“real risk of significant harm”**
- However, the BC Government has issued guidance to assist with assessing “significant harm” under FIPPA:
 - [Guidance on Mandatory Privacy Breach Notifications](#)


CLARK WILSON  27

27

Mandatory Breach Notification

Assessing “Significant Harm”

- The Federal PIPEDA legislation sets out relevant factors in assessing whether there is a “real risk of significant harm”:
 - The sensitivity of the personal information involved in the breach.
 - The probability that the personal information has been – is being – or will be misused.
- Also important to consider the context of the breach and the personal information involved

CLARK WILSON  28


28

Mandatory Breach Notification

Assessing “Significant Harm” (cont.)

Important factors to consider:

1. Nature of the data involved in the breach
2. Cause and extent of breach
3. How many affected by the breach?
4. Who is affected and what are the harms?


CLARK WILSON  29

29

Mandatory Breach Notification

Helpful Guidance

- Federal Privacy Commissioner
[What you need to know about mandatory reporting of breaches of security safeguards](#)
- BC Privacy Commissioner
[Privacy breaches: tools and resources for public bodies](#)
[Privacy Breaches: tool and resources for the private sector](#)
- Alberta Privacy Commissioner.
[Privacy Breach Response, Reporting and Notification \(webpage with various links\)](#)

CLARK WILSON  30

30

Mandatory Breach Notification

Notification

1. Key Considerations

- Legislation requires notification
- Contractual obligations require notification
- Contact law enforcement and obtain advice as to whether notification should be delayed in order not to impede a criminal investigation
- Direct notification preferred (i.e. by phone, letter or in person)
- Indirect notification where necessary to avoid further harm, unreasonable costs or contact information is lacking (i.e. by websites, posted notices or media reports)
- CPPA reforms include significant penalties for breaches and a new private right of action.

CLARK WILSON DATA SENTINEL 31

31

Mandatory Breach Notification

Notification (cont.)

2. What should be included in notification to affected individuals?

- Name of organization
- Date or period on which breach occurred
- Description of breach
- Description of personal information involved in the breach
- Steps the organization has taken or will take to control or reduce harm
- Steps that individual can take to reduce risk of harm
- Contact information that individual can use to obtain further information about the breach

CLARK WILSON DATA SENTINEL 32

32

Mandatory Breach Notification

Notification (cont.)

3. What should be included in notification to Privacy Commissioner?

- Name of organization
- Date or period on which breach occurred
- Description of personal information involved in the breach
- Number of individuals affected by the breach
- Steps the organization has taken or will take to control or reduce harm
- Steps the organization has taken or will take to notify affected individuals
- Contact information of person who can answer questions or provide information about the breach to the Commissioner

CLARK WILSON DATA SENTINEL 33

33

Privacy Breach Reporting Forms

- Federal – [PIPEDA Breach Report Form](#)
- BC PIPA – [Online Privacy Breach Report Form](#)
[Privacy Breach Checklist for private organizations](#)
- BC FIPPA – [Online Privacy Breach Report Form](#)
[Privacy Breach Checklist for Public Bodies](#)
- Alberta PIPA – [Privacy Breach Report Form](#)

CLARK WILSON DATA SENTINEL 34

34

Preventative Measures

Mark Rowan, CEO, Data Sentinel
416-570-6228 | mark@data-sentinel.com

CLARK WILSON DATA SENTINEL 35

35

Detection and Action	Containment and Prevention
<p>Assemble a Response Team: This team might include IT professionals, cybersecurity experts, legal counsel, PR and communications specialists, and relevant management personnel. If you don't have sufficient expertise in-house, you might need to hire external specialists.</p> <p>Engage a Forensic Investigator: A thorough forensic investigation will help you understand what happened, how it happened, and how the attacker accessed your network. This involves analyzing system logs, understanding patterns of behavior, and identifying the exploited vulnerabilities.</p> <p>Assess the Scope of the Breach: Understand what data was accessed or stolen. This might involve a detailed data investigation, knowing the type of data that was compromised, the affected individuals, and other sensitive data in critical step in preparation for disclosure.</p> <p>Identify the Source of the Breach: Use forensic evidence to identify the source of the breach. This could involve malware analysis, studying network logs, or analyzing any physical activity.</p> <p>Cooperate with Regulators, Law Enforcement: In cases where criminal activity is suspected, you will likely need to work with local or national law enforcement agencies. They can also help to investigate the breach and possibly identify the culprit.</p>	<p>Fix the Vulnerabilities: Once you know how the breach occurred, fix the identified vulnerabilities. This might involve patching software, tightening network security measures, or improving access controls.</p> <p>Improve Security Infrastructure: Depending on the nature of the breach, it may be necessary to invest in new security tools and technologies. This could involve better network monitoring tools, intrusion detection systems, or advanced encryption technologies.</p> <p>Data Governance and Data Privacy Programs: Review your policies and controls related to data access, and data privacy. If you don't have controls / programs - implement them. This could include stronger password requirements, two factor authentication, and limiting access to sensitive data.</p> <p>Train Employees: If the breach was caused by human error, it's important to provide additional training to your staff. Make sure they understand the latest threats and their role in maintaining the security of the organization.</p> <p>Conduct Regular Privacy / Security Audits: Regular audits of your IT systems, data, processes and policies can help identify any remaining vulnerabilities or compliance issues. Make, Ticks, Sensitive Data Audit, Pen testing will help identify weaknesses in your compliance and security posture.</p> <p>Establish a Disaster Recovery Plan: If you don't already have a disaster recovery plan, now is the time to establish one. This plan will provide a roadmap for recovering from future security incidents and minimizing downtime.</p>
<p>These steps should be tailored to the specifics of the breach and your organization. The goal is to understand the breach fully and take measures to prevent similar incidents in the future.</p>	

CLARK WILSON DATA SENTINEL 36

36

Data is The Target


Building walls is not enough:

- Minimize your sensitive data footprint
- Encrypt sensitive data
- Data Governance, Data Privacy, and Data Security in sync
- Education


CLARK WILSON DATA SENTINEL 37

37


QUESTIONS?



Scott Lamb
Partner, Clark Wilson LLP
604 643 3103
slamb@cwilson.com



Jeff Holowaychuk
Partner, Clark Wilson LLP
604 643 3194
jholowaychuk@cwilson.com




Mark Rowan
Chief Executive Officer, Data Sentinel Inc.
416 570 6028
mark@data-sentinel.com

These materials are necessarily of a general nature and do not take into consideration any specific matter, client or fact pattern.


CLARK WILSON DATA SENTINEL 38

38


BIOGRAPHIES



Scott Lamb, Partner, Clark Wilson LLP
604 643 3103 | slamb@cwilson.com
Scott Lamb is a senior partner at the law firm of Clark Wilson LLP. He is the Chair of the Privacy Law Practice Group, Co-Chair of the Higher Learning Practice Group at Clark Wilson and is a member of Clark Wilson's Technology and Intellectual Property Practice Group. Scott has practiced in the area of privacy law since 2004. He has acted as legal counsel for clients in enquiries and investigations before the Privacy Commissioner of British Columbia as well as with respect to freedom of information (FOI) requests. Scott also provides legal advice with respect to privacy law compliance and the drafting and negotiation of privacy policies, contracts and related documentation.



Jeff Holowaychuk, Partner, Clark Wilson LLP
604 643 3194 | jholowaychuk@cwilson.com
Jeff Holowaychuk is a partner at Clark Wilson LLP with a practice in technology and privacy law. Jeff works closely with a variety of public bodies and private sector organizations on privacy compliance matters, including privacy management programs, data usage agreements, privacy impact assessments and other advisory work. He also advises clients on complex and strategic outsourcing, technology procurement and digital transformation projects, with expertise in licensing, cloud service and other technology agreements.



Mark Rowan, CEO, Data Sentinel Inc.
416 570 6028 | mark@data-sentinel.com
Mark Rowan is the CEO and co-founder of Data Sentinel, a technology company specializing in the automation of data privacy compliance and sensitive data management, based in Toronto, Ontario. Prior to co-founding Data Sentinel, Mark was the CEO of Stream Integration, a global data governance, data management, and data privacy firm. The roots of Mark's data management experience extend into IBM, where he managed a significant element of IBM's data management professional services business. At Data Sentinel, Mark is responsible for the overall vision, strategy and direction of the company, which has the goal of helping organizations reduce the cost and complexity of governing sensitive data. In addition to his work at Data Sentinel, Mark is an active member of the data governance and privacy community, and he is a regular speaker at industry conferences and events.

CLARK WILSON DATA SENTINEL 39

39
