

SMARTBLOCK LAW



PROFESSIONAL CORPORATION

<https://smartblocklaw.com>

Privacy Due Diligence, Breaches, and Artificial Intelligence

Legal Presentation by Chetan Phull
for Trovo Resources

August 12, 2020



Chetan Phull

Principal Lawyer



FOCUS & CLIENTS

Chetan Phull has a regulatory focus in blockchain, cryptocurrency, privacy, cybersecurity, artificial intelligence, and IT contracts.

He also litigates cases related to software, digital assets, online platforms, regulatory investigations, online defamation, and cyber insurance. His litigation experience includes trials, applications, motions, and appeals, with upwards of \$40 million in dispute.

Chetan services a diverse range of sophisticated clients including public companies, financial institutions, investment firms, large private corporations, and high net worth crypto investors.

LAW BOOKS & ARTICLES

Chetan is the author of [Big Data Law in Canada](#), an 11-chapter book that critically examines various areas of law affecting data-driven enterprises.

He has also authored several [compilations](#) and [articles](#) on blockchain and virtual asset regulation, spanning [securities](#), [commercial transactions](#), [banking](#), [taxation](#), and [digital asset litigation](#).

Chetan also has publications appearing in the [Journal of International Arbitration](#), and the [Journal of International Banking Law & Regulation](#). In addition, his work has been [translated into Thai](#) by the Thai Arbitration Institute.

SPEAKING ENGAGEMENTS

Chetan has delivered seminars on blockchain and privacy laws for the [Ontario Bar Association](#), [Osgoode Professional Development](#), the [BlockchainHub at York University](#), and the [Government of Dubai Legal Affairs Department](#).

He is a frequent speaker at industry events including the [MPWR Crypto Mining Summit](#), [Futurist Conference](#), [DEFCON Toronto](#), and [Cyber Tech & Risk](#).

CERTIFICATIONS

- Certified Information Privacy Professional – Canada and US (CIPP/C/US) (2019 & 2020)
- CipherTrace Certified Examiner (forensic cryptocurrency investigation) (2019)
- Called to the Bars of Ontario, New York State and Massachusetts (2013)

EDUCATION

- Clerkship, Nova Scotia Court of Appeal (2011-2012)
- Master of Laws, University College London (2010-2011)
- Juris Doctor, Queen's University (2007-2010)
- Bachelor of Music in Composition, University of Toronto (2003-2007)

SMARTBLOCK LAW



PROFESSIONAL CORPORATION

<https://smartblocklaw.com>

Firm Overview

We provide **LEGAL ADVICE** on blockchain, cryptocurrency, privacy, cybersecurity, artificial intelligence, and IT contracts.

We **LITIGATE** cases related to software, digital assets, online platforms, regulatory investigations, online defamation, and cyber insurance.

We are **THOUGHT LEADERS** in the laws of data and digital activity. See our free legal resources, frequent speaking engagements, and regular media interviews.

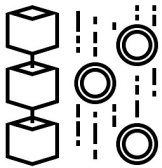
SMARTBLOCK LAW



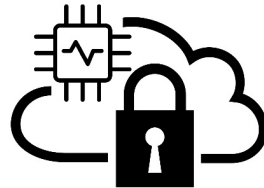
PROFESSIONAL CORPORATION

<https://smartblocklaw.com>

Expertise



*Blockchain &
Cryptocurrency*



*Data Privacy &
Artificial Intelligence*



*IT, Software &
Internet Contracts*



*Litigation &
Arbitration*

Legal Resources



[Big Data Law in Canada](#)



[Data Privacy & Blockchain Law Slideshow](#)

[\(March 2019\)](#)



[Smartblock Law Guide to Security Tokens,
OTC Trades, Prospectus Exemptions, and
Registration](#)



[Smartblock Law Guide to Cryptocurrency
Contracts, Litigation, Monetary Instruments,
and Financial Institution Regulations in
Canada](#)

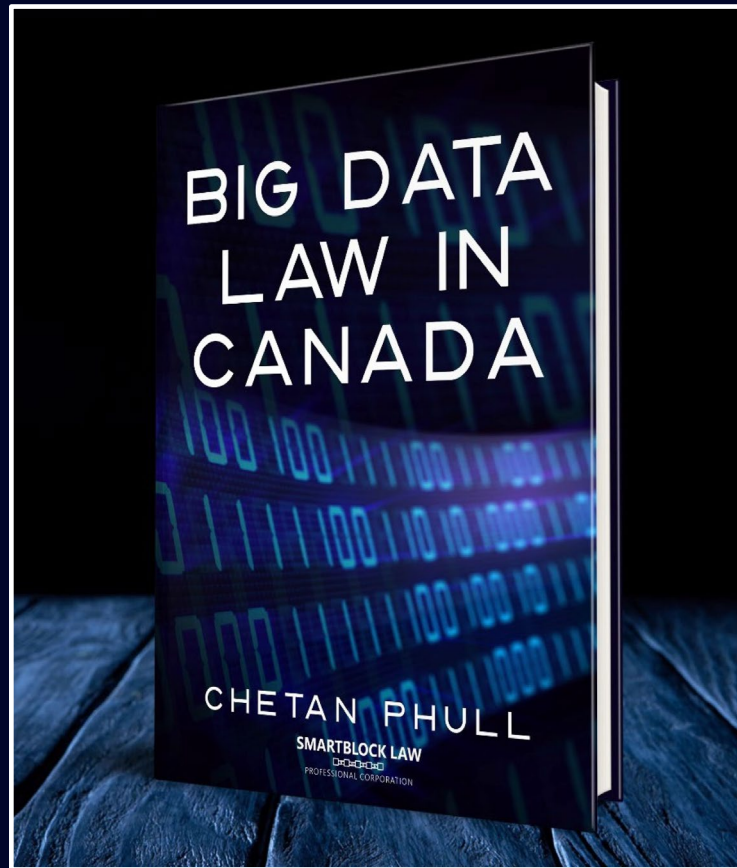


[Smartblock Law Crypto-Tax Primer](#)



[Other Articles](#)

Big Data Law In Canada



Online: FREE

(smartblocklaw.com)

Paperback: \$59.95

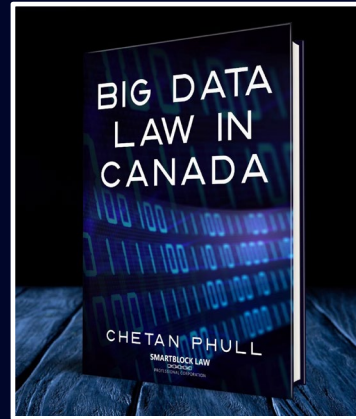
(Amazon.ca)

SMARTBLOCK LAW

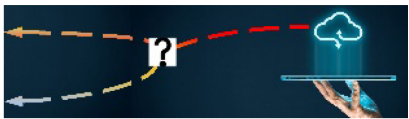


www.smartblocklaw.com

Big Data Law In Canada



1



**DEALING WITH
DATA GOVERNANCE
LEGAL ISSUES**

2



**THE FRAMEWORK
OF BIG DATA LAW IN
CANADA, AND ITS
PRIVACY LAW CORE**

3



**CYBERSECURITY
LEGAL STANDARDS
AND BASELINE
CONTROLS**

4



**DATA BREACHES –
PLANNING,
REACTING, AND
LITIGATING**

5



**DIGITAL
AUTHENTICATION**

6



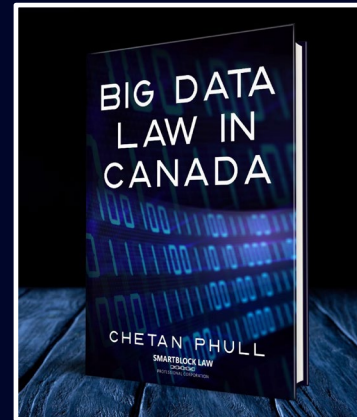
**CANADIAN ANTI-
SPAM LEGISLATION
("CASL")**

SMARTBLOCK LAW



www.smartblocklaw.com

Big Data Law In Canada



7



THE RIGHT TO BE FORGOTTEN / RIGHT OF ERASURE

8



TRANS-BORDER DATA FLOWS AND DATA LOCALIZATION REQUIREMENTS

9



GOVERNMENT SURVEILLANCE, CYBERSECURITY AND CYBER OPERATIONS

10



ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING SYSTEMS

11



BIG DATA AND COMPETITION / ANTI-TRUST LAW

SMARTBLOCK LAW



www.smartblocklaw.com

Disclaimer

- The material shared during this seminar is offered as general information only, not legal advice.
- Chetan Phull, Smartblock Law Professional Corporation, and its employees, contractors, and agents, as well as the event organizers, are **not** responsible for your reliance on the information shared during this presentation.
- You should obtain formal legal advice particular to your situation.

Copyright

This slideshow is copyright 2017-2020 Smartblock Law Professional Corporation. All Rights Reserved.

SMARTBLOCK LAW



www.smartblocklaw.com

Agenda

- (1) Privacy Law Framework in Canada, and Latest International Developments.
- (2) Breach Law,
- (3) Regulation of Artificial Intelligence.

Agenda

(1) Privacy Law Framework in Canada, and Latest International Developments.

(2) Breach Law,

(3) Regulation of Artificial Intelligence.

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
 - Different jurisdictions
 - PIPEDA is federal;
 - BC has a provincial *Personal Information Protection Act*;
 - AB has a provincial *Personal Information Protection Act*;
 - QB has *An Act Respecting the Protection of Personal Information in the Private Sector*;
 - *Municipal Freedom of Information and Protection of Privacy Act* (ON);
 - Various international treaties (discussed later).

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
 - Different industries – for example, health
 - ON has *Personal Health Information Protection Act*;
 - NB has *Personal Health Information Privacy and Access Act*;
 - NS has *Personal Health Information Act*;
 - Nfld has *Personal Health Information Act*.

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
 - Different industries – for example, the financial and investment sectors
 - *Bank Act* (federal);
 - *Trust and Loan Companies Act* (federal);
 - *Insurance Act* (ON);
 - *OSFI Guidelines*;
 - *CSA, IIROC, and MFDA for the capital markets.*

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
 - Public vs. Private sectors
 - PIPEDA covers employee information of federally regulated organizations (e.g. banks and telecom companies), and ***personal information in the course of commercial activities that do not have substantially similar legislation (i.e. all provinces except AB, BC, and QC).***
 - Federal public sector is covered by the *Privacy Act* (federal).

Data Privacy & Cybersecurity: Legal Framework

- There are also Criminal Code provisions to keep in mind:
 - **Criminal Code, s. 184:** using a device willfully to intercept a private communication without the express or implied consent of the originators or intended recipient; and
 - **Criminal Code, at s.342.1:** intercepting fraudulently and without colour of right any function of a computer system.

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is next covered by statutory torts for breach of privacy without damages:
 - Only in British Columbia, Manitoba, Newfoundland and Saskatchewan.
- Let's not forget CASL:
 - Several prohibitions against installing computer programs without consent.

Data Privacy & Cybersecurity: Legal Framework

- Finally, private common law rights of actions in:
 - tort;
 - negligence;
 - breach of contract;
 - breach of consumer protection legislation;
 - breach of trust/fiduciary duty;
 - breach of privacy;
 - intrusion upon seclusion; and
 - unjust enrichment.

Latest International Developments

- Europe -> GDPR
- California -> CCPA (persuasive across the U.S.)
- Quebec -> Bill 64 (not international, but influenced by the above)
- EU-US Privacy Shield invalidation on July 16, 2020.
- How does the Privacy Shield affect Canadian Business? [See here.](#)

Agenda

(1) Privacy Law Framework in Canada, and Latest International Developments.

(2) Breach Law,

(3) Regulation of Artificial Intelligence.

Data Privacy & Cybersecurity: Cybersecurity Standards and Management of Third Party Risk

- PIPEDA states:

“Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

...

“The methods of protection shall include

...

“(c) technological measures, for example, the use of encryption.”

(See [ss.4.7](#) and [4.7.3\(c\)](#).)

Data protection duties

“Private organizations are responsible for personal information under their control. They are obligated to implement security safeguards appropriate to the sensitivity of such information. These obligations apply to data controllers and processors alike. Moreover, the principal data controller remains responsible for the data handling practices of any third-party processor it contracts with.”

Chetan Phull, *Big Data Law in Canada* at [23](#).

Data protection duties

First step:

Designate an officer responsible for privacy compliance.

[See *PIPEDA*, Sch. 1, Principle 4.1.]

Second step:

Perform a privacy impact assessment (“PIA”), with respect to any personal data that could arguably be within the organization’s control, either directly or indirectly.

[*Directive on Privacy Impact Assessment*]

Data protection duties

The privacy officer should use the PIA to:

1. assess privacy risks;
2. assess the present level of privacy compliance;
and
3. determine additionally required steps.

Data protection duties

Risk assessment and action plans should be undertaken with a focus on the following ten fundamental privacy principles found in legislation:

1. Accountability;
2. Identifying Purpose for Collection;
3. Consent;
4. Limiting Collection;
5. Limiting Use, Disclosure, and Retention;
6. Accuracy;
7. Safeguards;
8. Openness;
9. Individual Access; and
10. Challenging Compliance.

[See PIPEDA, Sch. 1.]

Data Privacy & Cybersecurity: Reacting to Breaches

- New rule as of November 2018:

Private organizations must keep records of all security breaches exposing personal information, for 2 years after each breach is discovered.

- This rule stems from PIPEDA (federal legislation).
- Failure to report can result in a fine upwards of \$100,000.

Data Privacy & Cybersecurity: Reacting to Breaches

- When do the breach requirements kick in?
- Think RROSH: “real risk of significant harm” to an individual

Agenda

(1) Privacy Law Framework in Canada, and Latest International Developments.

(2) Breach Law,

(3) Regulation of Artificial Intelligence.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- Issues for consumers in AI and data collection/processing:
 - The processing of data, through computer code embedded in “smart devices” or pushed to a back-end, is not visible or otherwise tangible for consumers.
 - Users may not have control over data collection, data processing, or decision logic run by their mobile or IoT devices.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- As of April 1, 2019, Canada's [Directive on Automated Decision-Making](#) took effect.
- It emphasizes “core administrative law principles such as transparency, accountability, legality, and procedural fairness”, and is anticipated to evolve in order to stay relevant.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- CIO standard, called the *Ethical design and use of automated decision systems*, applies to both the public and private sector.
- Confusing application, and not a true set of minimum standards.
- Good intentions but poor execution.
- See my critical analysis of the CIO standard in:

Big Data Law in Canada, [Chapter 10](#): “Artificial Intelligence and Machine Learning Systems”.

SMARTBLOCK LAW



www.smartblocklaw.com

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- On January 28, 2020, the OPC released, “Proposals for ensuring appropriate regulation of artificial intelligence”
- “AI presents fundamental challenges to all foundational privacy principles as formulated in PIPEDA.” Examples:
 - Limited data collection?
 - How the information will be used ahead of time?
- Deadline for feedback was March 13, 2020. No further updates yet.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- **Proposal 1:** Create a definition of “AI” that falls within the definition of “processing”.
- **Proposal 2:** Human rights-based approach to AI.
- **Proposal 3:** A right to object to automated decision making.
- **Proposal 4:** Right to algorithmic transparency when subject to automated decision making.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- **Proposal 5:** Privacy-by-Design and Human-Rights-by-Design required for data collection and processing.
- **Proposal 6:** Compliance requirements with “purpose” and “data minimization” should be made realistic and effective.
- **Proposal 7:** When meaningful consent is not practical, legislation should provide alternatives for processing, and solutions to protect privacy.
- **Proposal 8:** Relaxed rules for non-identifiable data, and measures to protect against re-identification in such data.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- **Proposal 9:** Requirements for data and algorithmic traceability (further to the algorithmic transparency objective)
- **Proposal 10:** Requirement for demonstrable accountability for development and implementation of AI processing.
 - Note potential exposure for developers and operators.
- **Proposal 11:** Empower OPC to issue binding orders and fines.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- How will the courts handle AI?
- Ontario courts have promoted the use of artificial intelligence, at least with respect to lowering legal costs.
 - *Cass v. 1410088 Ontario Inc.*, 2018 ONSC 6959 at [para 34](#) (CanLII):

[10] My own view is that the hours spent on legal research is recoverable both as a component of counsel fee and as a disbursement. The reality is that computer-assisted legal research is a necessity for the contemporary practice of law and computer assisted legal research is here to stay with further advances in artificial intelligence to be anticipated and to be encouraged. Properly done, computer assisted legal research provides a more comprehensive and more accurate answer to a legal question in shorter time than the conventional research methodologies, which, however, also remain useful and valuable. Provided that the expenditure both in terms of lawyer time and computer time is reasonable and appropriate for the particular legal problem, I regard computer-assisted legal research as recoverable counsel fee item and also a recoverable disbursement.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- How will the courts handle AI?
- Ontario courts have promoted the use of artificial intelligence, at least with respect to lowering legal costs.
 - *Drummond v. The Cadillac Fairview Corp. Ltd.*, 2018 ONSC 5350 at [para. 10](#) (CanLII):

[34] All in all, whatever this “research” was would be well within the preparation for the motion. There was no need for outsider or third party research. If artificial intelligence sources were employed, no doubt counsel’s preparation time would have been significantly reduced.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- See also the recent Australian case, [*Pintarich v Deputy Commissioner of Taxation*](#), [2018] FCAFC 79 (Fed. Ct. Aus.) at paras. 141-43, 151.
- This case provides a broader analysis of automated decision making.

FIN

SMARTBLOCK LAW



www.smartblocklaw.com

SMARTBLOCK LAW



PROFESSIONAL CORPORATION

<https://smartblocklaw.com>

info@smartblocklaw.com | 1-833-BIT-LAWS | 250 Yonge Street, Suite 2201 | Toronto, Ontario, M5B 2L7, Canada

