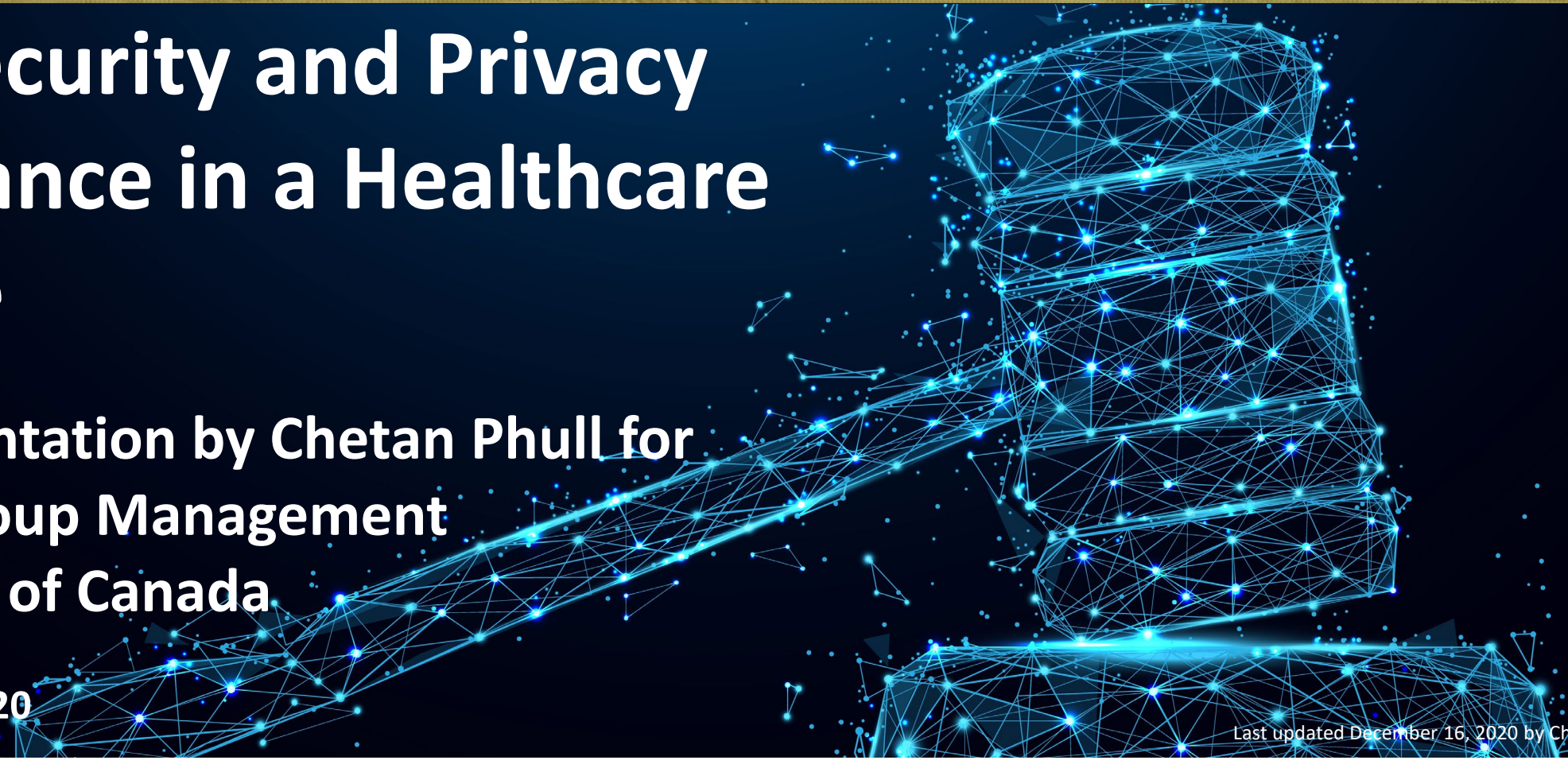
SMARTBLOCK LAW

PROFESSIONAL CORPORATION

https://smartblocklaw.com

Cybersecurity and Privacy Compliance in a Healthcare Practice



Legal Presentation by Chetan Phull for Medical Group Management Association of Canada

December 16, 2020

Last updated December 16, 2020 by Chetan Phull

Chetan Phull

***Principal Lawyer* – LLM, JD, CIPP/C/US**

SMARTBLOCK LAW
PROFESSIONAL CORPORATION

CERTIFICATIONS

- Certified Information Privacy Professional - Canada and US (CIPP/C/US) (2019 & 2020)
- CipherTrace Certified Examiner (blockchain forensics) (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)

FOCUS & CLIENTS

Chetan Phull has a focus in privacy, cybersecurity, blockchain, cryptocurrency, artificial intelligence, and SaaS & IT vendor contracts. His technology law practice with Smartblock Law P.C. will be transitioning to Deloitte Legal Canada LLP in January 2021.

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 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*, *digital asset litigation*, and decentralized liability.

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.

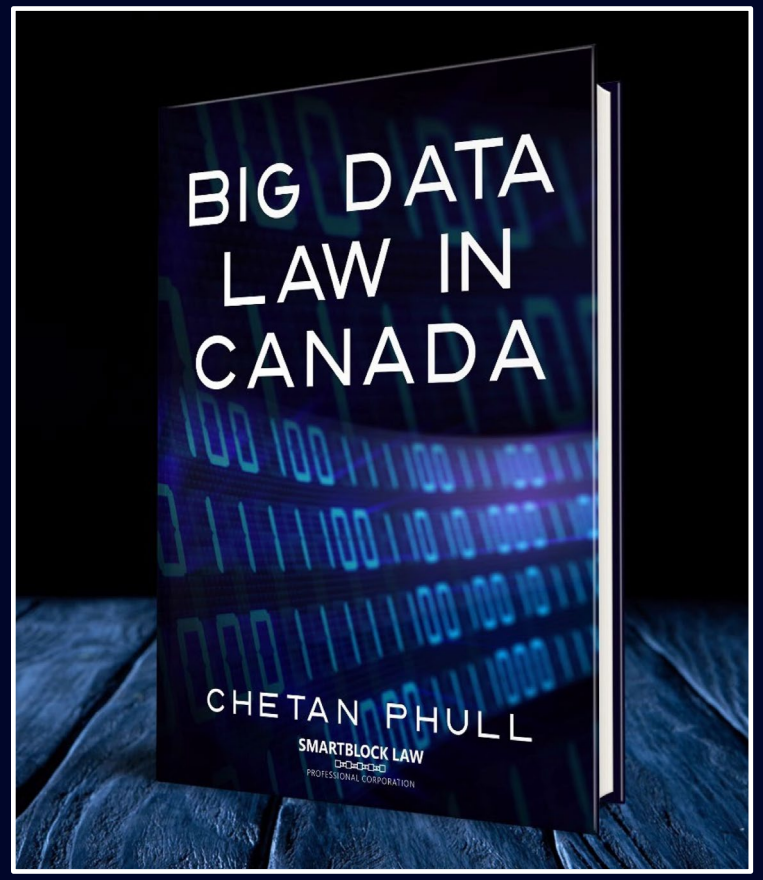
SPEAKING ENGAGEMENTS

Chetan has delivered seminars on blockchain and privacy laws for the *Ontario Bar Association*, *Osgoode Professional Development*, the *Medical Group Management Association of Canada*, 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*.

Last updated December 16, 2020 by Chetan Phull

Big Data Law In Canada



Online: FREE

(smartblocklaw.com)

Paperback: $59.95

(Amazon.ca)

Disclaimer

- The material shared within this slideshow 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

Agenda

(1) 10 Privacy Principles

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

(3) Ontario's *Personal Health Information Protection Act*

(4) Breach Notification & Reporting

Agenda

(1) 10 Privacy Principles

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

(3) Ontario's *Personal Health Information Protection Act*

(4) Breach Notification & Reporting

10 Privacy Principles from PIPEDA

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.

These ten privacy principles may appear conceptually simple. However, they are deceptively complicated to implement for compliance purposes.

10 Privacy Principles from PIPEDA

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.

Legislative developments are attempting to clarify these principles, in a manner that balances commercial and privacy interests.

Agenda

(1) 10 Privacy Principles

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

(3) Ontario's *Personal Health Information Protection Act*

(4) Breach Notification & Reporting

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
    - Different jurisdictions
        - *PIPEDA* and *Privacy Act* are federal (federal framework to be overhauled);
        - 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);
        - QB and ON are in the process of, respectively, passing and drafting new provincial privacy statutes;
        - Various international treaties (discussed later).

Data Privacy & Cybersecurity: Legal Framework

- Personal health information in certain provinces will exempt the application of PIPEDA.

- For example:

  - 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

- However, the main federal privacy statutes are in the process of being overhauled:
    - 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).***
        - ***But note Bill C-11 re Digital Charter Implementation Act, 2020*** *– overhauls PIPEDA; enacts Consumer Privacy Protection Act ("CPPA") and Personal Information and Data Protection Tribunal Act ("PIDPTA").*
    - **Federal public sector is covered by the *Privacy Act.***
        - Feedback for amendments due January 17, 2021.

Data Privacy & Cybersecurity: Legal Framework

What does the new federal legislation mean for provincial health privacy legislation?

PHIPA replaces PIPEDA with respect to health information custodians.

Will PHIPA replace the forthcoming *Consumer Privacy Protection Act*?

Or will health information custodians soon have two sets of privacy compliance rules to follow?

Data Privacy & Cybersecurity: Legal Framework

- The broader privacy law framework in Canada also includes *Criminal Code* provisions:

  - ***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

- There are also 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 action 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., not to be confused with Canada's forthcoming CPPA)
- EU-US Privacy Shield invalidation on July 16, 2020.
  - How does the Privacy Shield affect Canadian Business? See here.

Agenda

(1) 10 Privacy Principles

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

(3) Ontario's *Personal Health Information Protection Act*

(4) Breach Notification & Reporting

Privacy & Healthcare in Ontario

- PHIPA draws from the 10 privacy principles discussed earlier:

The purposes of this Act are,

(a) **to establish rules for the collection, use and disclosure of personal health information** about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care;

(b) to provide individuals with a **right of access** to personal health information about themselves, subject to limited and specific exceptions set out in this Act;

(c) to provide individuals with a **right to require the correction or amendment of personal health information** about themselves, subject to limited and specific exceptions set out in this Act;

(d) to provide for **independent review and resolution of complaints** with respect to personal health information; and

(e) to provide **effective remedies** for contraventions of this Act.

Privacy & Healthcare in Ontario

- PHIPA was last amended on March 25, 2020, with further tech-focused amendments to take place in future.

- Commissioner can impose administrative penalties for contravention of PHIPA or its regulations.
  - Up to $200,000 and one year's imprisonment for an individual, and $1 million for an organization.
  - Directors and officers can be liable regardless of whether the corporation is prosecuted or convicted.

Privacy & Healthcare in Ontario

- PHIPA's equivalent of data controllers are "health information custodians".
  - Definition of "health information custodians" includes "[a] health care practitioner or a person who operates a group practice of health care practitioners," long term care homes, retirement homes, pharmacies, labs, ambulance services, special care homes, and community or mental health centres, hospitals, and other prescribed persons under the regulations.
  - After upcoming amendments take effect, the definition will also include certain "health service providers", persons/entities on an "Ontario Health Team", and community health facilities.

Privacy & Healthcare in Ontario

- “Personal health information” under PHIPA is:
    - information that can be used toward identification of an individual,
    - in oral or recorded form,
    - relating to:
        - physical or mental health,
        - the provision of health care services,
        - insurance coverage,
        - donation of body parts,
        - health number, or
        - identification of a substitute decision maker.

Privacy & Healthcare in Ontario

- Patient consent under PHIPA.
  - Numerous consent provisions in PHIPA deal with permitted collection, use, and disclosure of PHI.
  - The issue of consent is complicated when substitute decision makers are involved.
  - Electronic health records get their own collection, use, and disclosure provisions.
- Once consent is established, fees may be charged for disclosing, or providing access to, personal health information.
  - Only “reasonable cost recovery” is permitted. (See PHIPA at ss.35(1)-(2), 54(10)-(11); PHIPA Decision 93 [2019] at paras. 41-49.)

Privacy & Healthcare in Ontario

- New PHIPA provisions as of March 2020:
  - In certain circumstances, patient consent must be given for the custodian to verify the patient's ID through patient's health card number.
  - Patients now also have a right to access their records in electronic form.

Privacy & Healthcare in Ontario

Future tech-specific amendments in PHIPA:

- Mandatory electronic audit logs for every instance of read/write access – must be provided to Commissioner on request.
- Further de-identification rules by regulation.
- Non-custodian electronic service providers are contemplated to become subject to PHIPA.

Agenda

(1) 10 Privacy Principles

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

(3) Ontario's *Personal Health Information Protection Act*

(4) Breach Notification & Reporting

Breach Notification & Reporting

- Breach requirements in PHIPA:

  (a)notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and

  (b)include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

- Notice to Commissioner is required if personal health information was used, accessed, or disclosed without authority, or was stolen.

- Notice to Commissioner is also required where disclosure of PHI is sensitive, or in large volumes, or involving many individuals, or where more than one custodian or agent is responsible.

Breach Notification & Reporting

- PIPEDA and CPPA rule re breach records:
  - Private organizations must keep records of all security breaches exposing personal information.
- Breach records must be maintained for 2 years under PIPEDA regulations.
  - It is not yet certain what the breach record maintenance requirement is under the CPPA.
- A breach-reporting requirement is triggered upon “real risk of significant harm” to an individual.

Security Safeguards

- PHIPA's security provision:
  - *12 (1) A health information custodian shall take **steps that are reasonable in the circumstances** to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.*

Security Safeguards

- 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).)

In Closing …

What do strengthened privacy laws mean for health information custodians*?*

Custodians will need to maximize their compliance profiles by:

1. reviewing their data-handling operations;
2. reviewing their technology and upgrade policies;
3. reviewing their contracts with third party electronic service providers;
4. staying updated on developing privacy laws and norms.

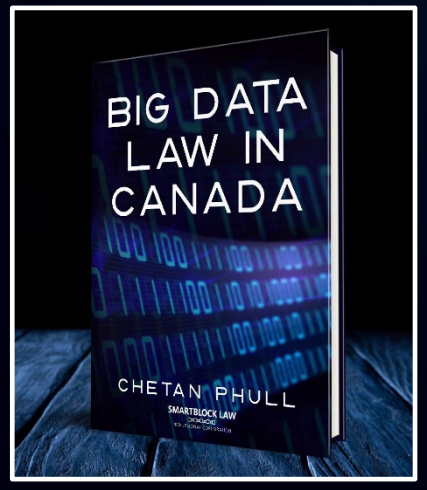
FIN

SMARTBLOCK LAW

PROFESSIONAL CORPORATION

https://smartblocklaw.com

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



Online: FREE (smartblocklaw.com)

Paperback: $59.95 (Amazon.ca)