Tips and Tech Solutions for Crossing the Border With Client Data

OBA Professional Development
Packing Your Digital Suitcase – Understanding Your Professional Obligations When Client Data Crosses Borders
April 13, 2018

OZIEL LAW
BUSINESS AND TECHNOLOGY LAW

Allan Oziel
Oziel Law
☎ 416.900.0882
✉ aoziel@oziellaw.ca
@allanoziel
www.oziellaw.ca

ALLAN OZIEL

Founder of Oziel Law, a boutique business, technology and IP law firm in Toronto

Co-Chair of Law Society of Upper Canada (LSUC) Solo and Small Firm Conference

Director and Treasurer of the Canadian Technology Law Association (Can-Tech Law)

Regular writer, speaker, and contributor on technology law, legal technology, and small firm topics

PIPEDA PRINCIPLES

RETAINER AGREEMENT AND PRIVACY POLICY

CLOUD STORAGE

ENCRYPTION

USING BURNERS AND OTHER EXTREME METHODS

COMING BACK INTO CANADA

PIPEDA PRINCIPLES

- Organization is responsible for personal information in its possession.
- Safeguards to be used will depend on the sensitivity of the information collected

PIPEDA PRINCIPLES

OPC – Guideline on Protecting Personal Data Across Borders

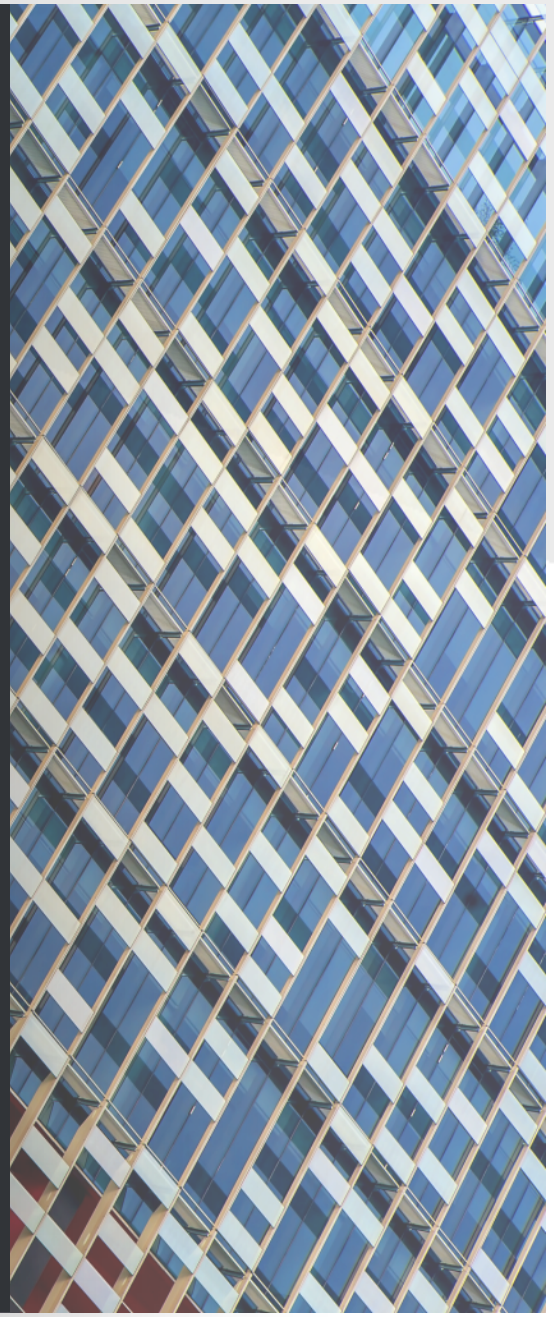
- Key is to balance protection of personal information with the business necessity.
- Requirement on organization to understand implications of transferring data including risk of access by law enforcement and national security authorities.
- Risk management program needs to be adjusted given the political, economic and social conditions at the time.

RETAINER AGREEMENT AND PRIVACY POLICY

- Under the PIPEDA Principles, “knowledge and consent” are required – Clients must have knowledge of how the information will be collected, used and disclosed and must provide sufficient consent.

- Retainer Agreements and Privacy Policies are often used to communicate this information and request consent.

- Privacy Policy should also advise if client data will be transferred outside of Canada.



CLOUD STORAGE

- **US Customs and Border Protection (USCBP) Directive updated January 4, 2018.**
- **Confirmed that passcodes and other means of access can be requested but only to search what is resident on the device.**
- **Formal exclusion of cloud-based information.**

CLOUD STORAGE

- In a “basic search”, access to information stored on a remote server or cloud will not be requested.
- Beware of syncing!
- Consider keeping all client data accessible only through logging into cloud server or e-mail server or using selective sync options.
- Log out of cloud providers, e-mail and social media.
- Turn on airplane mode so that your device cannot connect to the internet.

- Consider encrypting particularly sensitive information.
- Windows devices come with BitLocker encryption capability.
- Mac devices can be encrypted using Apple’s FileVault.
- Both iPhones and Androids are encrypted by default but accessed through passcodes and other means of access.

ENCRYPTION

USING BURNERS AND OTHER EXTREME METHODS

For lawyers with extremely sensitive client data, consider:

- “Burner devices” – separate devices just for travelling that don’t contain client information locally.

- Two Factor Authentication for certain apps – passcode sent to a phone or SIM card that is couriered to the destination.

Concern is that these measures may arouse suspicion.

COMING BACK INTO CANADA

- S.99 of the Customs Act permits a “non-intrusive search of goods”
- Definition of “Goods” is broad
- Canada also has a policy but it’s harder to find! (**CBSA Operational Bulletin** PRG 2015-31 “Examination of Digital Devices and Media at Port of Entry”)
- Officers must disable wireless and internet connectivity
- Only examine what is on the device and not read e-mails **“unless information is already downloaded and has been opened (marked as read)”**

OZIEL LAW
BUSINESS AND TECHNOLOGY LAW

ALLAN OZIEL

Oziel Law

☎ 416.900.0882

✉ aoziel@oziellaw.ca

@allanoziel

www.oziellaw.ca

OZIEL LAW

BUSINESS AND TECHNOLOGY LAW