TRAVELLING WITH MOBILE DEVICES

On Monday, September 18, 2017, Canada's Privacy Commissioner, Daniel Therrien, advised a House of Commons committee that U.S. Customs officers can look at mobile devices and even demand passwords under American law. Unless you are unconcerned about U.S. officers accessing your mobile devices, Commissioner Therrien advised that you should not take them across the U.S. border.

If you are an employee of a public body as defined in the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA,* 2015) and/or a custodian as defined in *Personal Health Information Act* (*PHIA*), you must consider more than the privacy of your own personal information when travelling with a mobile device issued to you by your employer. If that device has *personal information* and/or *personal health information* stored on it (or provides access to same) you have legal obligations to protect the privacy of that information.

If you are the head of a public body as defined in the *ATIPPA, 2015* and/or a custodian as defined in *PHIA*, you are legally obliged to ensure that reasonable safeguards are in place to protect the privacy of personal information and/or personal health information (as those terms are defined in legislation). At a minimum, this requires that you establish and communicate to employees' your organizations policies regarding travelling while in possession of mobile devices they have been issued in the course of their employment. Those policies should prohibit carrying personal information or personal health information on electronic devices while travelling.

Employees travelling with personal information and/or personal health information on a device should be aware that border officials may ignore claims of privacy and legal duties pursuant to the *ATIPPA, 2015* and/or *PHIA*. As such, you should carefully consider whether you might be risking exposure of personal information and/or personal health information to foreign government officials when crossing borders and take appropriate steps before travelling.

While both the *ATIPPA, 2015* and *PHIA* permit disclosures required by law, it is the position of the Newfoundland and Labrador Office of the Information and Privacy Commissioner (OIPC) that this is limited to Canadian law and excludes knowingly creating the potential for disclosure of personal information and/or personal health information to foreign government officials.

In terms of policies and procedures, the following suggestions represent some measures that may be considered:

- Ensure that all mobile devices are encrypted. This should be done regardless of travel status as mobile devices can be lost, stolen or otherwise misplaced during the course of day to day activities;

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

- Prohibit employees from carrying employer issued mobile devices when travelling to the U.S. for personal reasons;
- Minimize the amount of personal information and/or personal health information on mobile devices prior to travelling by backing up data on an external hard drive or other method. Leave the hard drive or other device in Canada. This not only protects privacy but ensures that the data remains accessible to the public body should the mobile device be seized by foreign government officials;
- If deleting files prior to travelling, do not simply move them to the trash folder, delete them completely;
- Maintain clean laptops (or hard drives) and phones that can be issued to employees travelling to the U.S. for work purposes; and
- Advise employees that in dealing with U.S. Customs officers or other foreign officials they cannot engage in obstructive behavior or be untruthful in responding to their questions. Employees must also be aware that refusal to provide passwords or to allow access to mobile devices can result in denial of entry into the U.S. and that mobile devices can be seized at the border.

If you allow employees to use their personal devices to conduct the business of a public body and/or custodian the same considerations apply and would then encompass both work and personal travel of employees. The practice of allowing employees to use their personal devices for business purposes, even with stringent safeguards, carries additional risks of unauthorized disclosure and further complicates crossing the U.S. border.