

SEARCH AND SEIZURE OF DIGITAL DEVICES

*NADER R. HASAN
STOCKWOODS LLP
AUGUST 2015*

Digital Search and Seizure

- ▣ “Territorial” versus “Informational” Privacy
- ▣ Reasonable Expectation of Privacy in Digital Devices
- ▣ Warrant Requirement
- ▣ Exceptions to the Warrant Requirement
- ▣ Online Anonymity



Reasonable Expectation of Privacy in Digital Devices

- ▣ “It is difficult to imagine a search more intrusive, extensive, or invasive of one’s privacy than the search and seizure of a personal computer.”

- *R. v. Morelli*, [2010] 1 SCR 253 at para. 2 per Fish J.

Reasonable Expectation of Privacy in Digital Devices

- ▣ “First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created....”

- *R. v. Morelli*, [2010] 1 SCR 253 at para. 3 per Fish J.

Reasonable Expectation of Privacy in Digital Devices

- ▣ “...The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident.”

- *R. v. Morelli*, [2010] 1 SCR 253 at para. 3 per Fish J.

Amount of Data Stored on a Computer Is Staggering

- ▣ For less than \$100, anyone can purchase a computer hard drive with storage capacity of one terabyte (1000 GB).
- ▣ 1000 GB = 500 million pages of text = amount of information contained in all of the books on twelve floors of an academic library!

The Computer Stores Private and Intimate Information

- ▣ Digital information often “falls at the very heart of the ‘biographical core’ protected by s. 8 of the *Charter*.”
- ▣ Virtually every aspect of one’s private life is consolidated into one’s computer, including:
 - Intimate correspondence;
 - Details of our financial, medical, and personal situations;
 - Internet search histories.

Lack of Control Over What Is Stored

- ▣ The computer is a “fastidious record keeper.”
- ▣ Computers generate information that is often unknown to the user, which tracks information about who created a document, on what date or who visited a given website at a particular time (“meta-data”).
- ▣ Cell phones, in addition, track geo-location points.

No “Delete” Button

- ▣ There is no such thing as a “DELETE” button!



VS.



The Interconnectedness of Computers

- ▣ A computer is not a stand-alone entity.
- ▣ It is a portal into a virtual world exponentially larger than the computer itself.
- ▣ Intermingling of data and third-party privacy interests.

R. v. Cole,
[2012] 3 S.C.R. 34

- ▣ Accused teacher did not own the school-issued laptop.
- ▣ School policy permitted incidental personal use.
- ▣ The accused used the laptop for personal use (e-mails, photographs).
- ▣ Does the accused have a reasonable expectation of privacy in the school-owned laptop?

The Warrant Requirement

- ▣ Recall: Where a reasonable expectation of privacy exists, a warrantless search is *presumptively* unreasonable.

R. v. Cole,
[2012] 3 S.C.R. 34

- ▣ Information stored on the computer “falls at the very heart of the ‘biographical core’ protected by s. 8 of the *Charter*.”
- ▣ Therefore ...
 - a reasonable expectation of privacy exists; and
 - Police need a warrant to search.

R. v. Cole,
[2012] 3 S.C.R. 34 at para. 65

“The police may well have been authorized to take physical control of the laptop and CD temporarily, and for the limited purpose of safeguarding potential evidence of a crime until a search warrant could be obtained.”

R. v. Vu, [2013] 3 S.C.R. 657

- ▣ Issue: Do police need *specific* authorization to search a computer?
- ▣ “Computers differ in important ways from the receptacles governed by the traditional framework....”
- ▣ Therefore, police need *specific, prior* authorization (a search warrant) to search a computer or cell phone.

R. v. Fearon, [2014] 3 S.C.R. 621

- ▣ Issue: Can the police search a cell phone without a warrant upon arrest of a suspect?



What's in a Smart Phone?

Example: A smart phone search revealed...

- 104 call logs;
- 8 passwords;
- 422 text messages;
- 659 geolocation points, including 227 cell towers and 403 WiFi networks with which the cell phone had previously connected; and
- 10,149 data files of audio, pictures, text and videos, 378 of them deleted.

Reference: ACLU, "New Document Sheds Light on Government's Ability to Search iPhones"

R. v. Fearon, [2014] 3 S.C.R. 621

- ▣ Police can conduct a limited warrantless search of the arrestee's cell phone, provided that:
 - The arrest is lawful.
 - The search is narrowly tailored to the legitimate purposes of a SITA:
 - ▣ Ensuring the safety of the police and the public;
 - ▣ Protection of evidence from destruction; and
 - ▣ Discovery of evidence that can be used at trial.
 - The police keep a detailed record of their search.

R. v. Spencer, [2014] 2 S.C.R. 212

- ▣ Police obtained Internet subscriber's name and address from ISP without a warrant.
- ▣ Accused argued that this violated s. 8 of the *Charter*.
- ▣ Crown argued that there is no privacy in a name and address.
- ▣ Right to “online anonymity”: people should have a right to act in the virtual world with some measure of freedom from identification and surveillance.

QUESTIONS?

Contact:

Nader R. Hasan

www.stockwoods.ca | naderh@stockwoods.ca