S E R V I N G C A N A D I A N S

DEPARTMENT OF JUSTICE

Emails: Considerations for Criminal Law Policy

Department of Justice, Canada

March 2005

Background

- Email goes back to the earlier days of the Internet;
- In some countries, it has become one of the most common ways in which persons communicate;
- Many forms of Internet communications have been broadly adopted:
  - E- commerce
  - Electronic banking
  - Web surfing, etc.
- Email is a form of evidence that police will increasingly rely upon in the future.

Legal issues: Interception or Seizure?

- Current law allows for interception of private communications and search and seizure of data under different regimes;
- Considering email communications are analogous to both telephone communications and letters, how should law enforcement obtain them?
  - Search and seizure warrant (e.g., letters and data)
  - Interception order (e.g., phone communications)
- Most countries, including Canada, have more significant safeguards for the obtaining of interception orders than for the obtaining of search warrants.

Legal Issues: Interception or Seizure? (cont.)

Technically, it is possible to acquire an email at several locations:

1a. During input at the keyboard of the sender;

1b. While message is stored on sender's computer;

2. During transmission between the sender's computer and the mail server of his ISP;

3. During temporary storage for processing on the server of the sender's ISP;

4. During the transmission between the sender's ISP and the recipient's ISP;

5. During temporary storage at the mailbox server of the recipient's ISP;

6a. During the reception by the recipient of the sender's message: transit from recipient's mailbox server to recipient;

6.b Message under recipient's control (temporary or permanent storage).

Legal Issues: Interception or Seizure? (cont.)

- Probably interception for 1a, 2, 4 and 6a;
- Probably seizure when email is located on the computer system;
- What about when the email is at either the sender or recipient's ISP?
  - Should an interception only be used when the email is actually "in transit" and not while it is "stored"?
  - Does the email cease to be a private communication because it is stored in a location?

Voice & Text: Differences & Similarities

- The main difference between voice and written communications appears to be ephemerality (the question of an intentional record);
- However, the raw material of a text or a voice transmitted on a network is likely to be similar, first because the communication is digitized; second because more and more service providers migrate to packet mode delivery for all forms of communication;
- Both voice and text can be sent by a personal computer just as both can be sent by a cell phone;
- **Do voice and text communications attract the same reasonable expectation of privacy?**

Reasonable Expectation of Privacy

- The Current *Criminal Code* definition of “private communication” provides that a communication is private when it is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any other person than the person intended by the originator to receive it;
- Courts have stated that reasonable expectation of privacy is an objective standard;
- Some individuals argue that email does not attract a reasonable expectation of privacy because it is easy to intercept or by nature of the technology it is always being intercepted (given definition of “intercept” and the nature of store-and-forward technologies as such);
- Consider 3 hypothetical scenarios:
  - Interception by personnel accessing mail servers
  - Interception in a large corporation
  - Interception by neighbours

1. Interception by Mail Server Personnel

- One argument is that an email passes through multiple mail servers (e.g., at sender's ISP and recipient's ISP, possibly relays in between) and can be intercepted at these points by personnel operating those servers or relays;
- In the world of voice telephony, by analogy, it is possible for personnel with access to switching equipment or curb-side pedestals to intercept phone calls: this did not diminish expectation of privacy;
- In fact, it led to the exemption in s.184(2)(c) – some other exemptions in s.184(2) follow similar rationale.

2. Interception in Large Corporation

- Excluding informatics personnel, is it objectively reasonable to believe that anyone in a corporation could intercept the email of someone else in that corporation?
- Knowing about the existence of packet sniffers does not mean knowing how to deploy one in the real world;
- Those that would know how might not be able to load a packet sniffer if the company had even minimal access rights preventing the local desktops from installing software
- If they could load a sniffer the location where it is loaded is significant: they might only acquire some corporate email but there could be constraints on acquiring other corporate email (different mail servers, different LAN segments, etc.).

3. Intercepting Your Neighbour?

- Is it easy for the average Canadian to intercept their neighbour's email?
- The simple fact of different Internet access providers serving the same neighbourhood raises an obstacle
- The fact that some teenage hackers could hack a mail server should not diminish an objective expectation of privacy;
- It is possible for someone to break and enter into a home and plant a home-made or store bought listening device but that does not diminish one's expectation of privacy in one's home.

Intercepting Email: Cell Phone Analogy

- If there were no objective standard for a reasonable expectation of privacy with respect to email, the situation would have to be analogous to the situation of analog cell phones;
- Email transmission is similar to telephony:
  - often it is wireline and the risks of interception are not dissimilar;
  - sometimes it is broadcast (wireless LANs or WiFi), which may introduce analogous circumstances of diminished expectation of privacy with respect to some radio-based telephony;
- If the WiFi security protocols (WPA, WPA2) are implemented, then it would be equivalent to “radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it”.

Interception of Email - Other Countries

- United States
  - Acquisition of the contents of the communication must be contemporaneous with the communication;
  - Does not apply to the electronic storage of email or data prior to its receipt.
- United Kingdom
  - An interception occurs when a person intercepts a communication in the course of its transmission;
  - In the course of its transmission includes any time when it is stored on the transmission system for the intended recipient to collect or access it.

Interception of Email - Other Countries (cont.)

- Australia
  - Consists of listening to or recording, by any means, such a communication in its passage over a telecommunications system.
  - Communications temporarily stored during transit are considered in passage over a telecommunications system.
- New Zealand
  - Intercept includes to “hear, listen to, or record, monitor, or acquire the private communication while it is taking place”.

Situation in Canada

- Uncertainty as to the type of order required to obtain email;
- Currently, law enforcement obtaining intercept orders for email “in transit” and search warrants for “stored” email;
- In most cases, an email stored in the course of it’s transmission is acquired with a search warrant;
- Does an email communication cease to be private simply because it is stored?
- In contrast, a mail letter can be seized once delivered to the recipient’s mail box (or during transmission if delivered by a person other than Canada Post) – communications made by letter are not covered by the definition of “private communication” (oral communication or telecommunication).