Tackling Organized Crime through Electronic Surveillance

Presented at the 4th IAP North American and Caribbean Regional Conference
November, 2016

Judy Kliewer, General Counsel
Public Prosecution Service of Canada, Manitoba Regional Office
Topics

- Overview of Canadian Law
  - Coexisting Contexts - organized crime vs protection of privacy rights
  - Statutory Powers to conduct electronic surveillance
- Role of the Prosecutor in the Investigation
- Challenges for Law Enforcement
- Best Practices for using Electronic Evidence at Trial
Overview of Canadian law

The co-existing contexts
Increased concern over Criminal Organizations

- Recognize harm to society and threat to public safety and security; international reaches; difficulty to investigate and prosecute

- Legislation intended to make investigation and proof of crim orgs more flexible and penalties increased
Increasing protection of privacy in the electronic era

• Intercepting and recording private communications recognized as the “greatest leveler of human privacy ever known” in 1971

• Notion continues in the era of electronic communication, digital storage and access to the internet
The Privacy Context – Computer searches

“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... 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.”

Overview of Canadian law

Electronic Surveillance – statutory powers
Types of Authorities

- Interception of Private Communications
- Video surveillance in private places
- Electronic tracking of persons, transactions and things
- Capturing transmission data
- Production orders for historical records
- Other techniques for gathering electronic data that identifies people, associations, communication devices
Interception of Private Communication

• At least one party to the communication must be in Canada – jurisdictional issues

• What is “interception” requiring Authorization?
  – listen to, record or acquire a communication
  – acquire the substance, meaning or purport thereof

  • *R v Telus Communications Co*, 2013 SCC 16 (CanLII) - messages stored on service provider server
  • *R v Mills*, 2013 CanLII 74953  vs *R v Graff*, 2015 ABQB 415 (CanLII) – electronic messaging recorded by method of transmission
Video Observations

• What are circumstances creating expectation of privacy?
  – Continuum from public to private
  – Territorial vs informational
  – nature of the information vs what it tends to reveal...
Tracking transactions, things and persons

- “Reasonable Belief” standard to track people
- “Reasonable Suspicion” standard to track transactions and things
General Warrants – Other techniques

- Authorizes use of a technique or device to do something that is a “search” (engages an expectation of privacy) that provides information about the offence, for which there exists no other authorization
  - Electronic surveillance techniques not contemplated by any statutory provision
  - Necessary to consider terms and conditions to minimize intrusion to extent necessary
Production and Preservation Orders

• Permit production of historical records
  – Trace communications
  – Transmission data
  – Tracking data
  – Financial data
  – Any other records

• Preservation Orders – “do not delete”
Role of the Prosecutor in the Investigation
Role of the Crown in Investigations

- Investigating agency has autonomy in the investigation, but the Crown assists in ensuring the investigation becomes a viable prosecution.
- Statute requires Crown to bring application for Wiretap authorization.
- Wiretap investigations, especially Criminal Organization investigations, will require Crown involvement and advice in all ancillary warrant applications made by police.
The Prosecutor as Minister of Justice

- Duty to Act in the public interest - balance privacy rights with the need to have law enforcement solve crime.
  - Ensure “the best interests of the administration of justice”
  - Ensure financially and legally manageable prosecutions
  - Protect confidential informants, investigative techniques and solicitor client privilege
The Prosecutor as Gatekeeper

- **Gatekeeper** – ensure statutory preconditions are met
- **Screening** – ensure the materials put before the Judge meet a standard appropriate for judicial analysis
The Prosecutor’s Ethical Obligations

- Obligation not to mislead the Court on *ex parte* application – accurate, candid, comprehensive

  - *Canadian Bar Association Code of Professional Conduct*
The Prosecutor’s Role

• Legal advice

• Planning toward manageable prosecution(s)

• Reviewing warrant applications

• Overseeing Disclosure / preparing case for prosecution / protecting privilege.
Prosecutor’s Role in Providing Legal Advice

Anticipating the “right answer” in shifting and Uncertain Landscapes...

• Evolving technology
  – how to apply existing legislation?

• Evolving views on privacy
  – Territorial
  – Informational
  – Anonymity
  – Perceived invasiveness of particular surveillance techniques
Challenges for Law Enforcement

Technology and Jurisdiction
Evolution of telecommunication technologies:

- 1876 – Alexander Graham Bell invented the telephone system.
- 1876 – 1970 very little change in how telephone system works.

• Since 1980 the telecommunications industry has seen extraordinary changes and technological advances.

• Today telecommunications are increasingly internet based.
Jurisdiction Issues

Internet
• no national / territorial boundaries

Stored Data
• Off-shore Service Providers – non-treaty countries
• Finding the data through maze of off-shore proxy servers
Getting around Jurisdiction

- MLAT – too little too late?
  - Police to Police cooperation can be invaluable
  - Formal MLAT process between states takes time...
Technical Challenges for Law Enforcement

Technical Challenges
Technological Challenges

• Encryption
  – PGP-enabled BlackBerry and other smartphones
  – ‘The Snowden Effect’ = Encryption by default

• Anonymous Services / Authentication
  – Prepaid mobile phone cards
  – Exchangeable SIM cards
  – Public internet access
  – Unsecured private Wi-Fi networks
  – Software for anonymous communication (Tor onion routing)
Best Practices for Using Electronic Evidence
Disclosure

- Electronic
- Self-explanatory, user friendly
- No data dumps – analyzed by investigators; significant evidence highlighted
- Technical implementation information disclosed unless investigative technique privileged
- Vetted for informer, investigative and solicitor client privilege
Presenting Evidence in Court

• Aids to jury:
  – Transcripts of audio
  – Data reduced to charts, graphs and summaries to aid to the jury if allowed by court.
  – Computer functions used to highlight data
  – PowerPoint presentations to demonstrate navigation

• Have your analysts assist!
### Eg - Cell phone location data (excerpt)

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>First Cell</th>
<th>Last Cell</th>
</tr>
</thead>
<tbody>
<tr>
<td>25-Apr-14 4:26:52 PM</td>
<td>302720F2A8F804</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:27:30 PM</td>
<td>302720F2A8F804</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:29:51 PM</td>
<td>302720F2A8AE1D</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:33:48 PM</td>
<td>302720F2A8AE19</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:34:00 PM</td>
<td>302720F2A8AE19</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:35:42 PM</td>
<td>302720F2A8AE19</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:35:54 PM</td>
<td>302720F2A8AE19</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:37:26 PM</td>
<td>302720F2A8AE1D</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:38:06 PM</td>
<td>302720F2A8AE1D</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:39:21 PM</td>
<td>302720F2A8AE29</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:40:00 PM</td>
<td>302720F2A8AE19</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 4:56:41 PM</td>
<td>302720F2A8AE18</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 6:01:02 PM</td>
<td>302720F2A8B0A0</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 5:05:11 PM</td>
<td>302720F618AD6A</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 7:11:21 PM</td>
<td>302720F230C746</td>
<td></td>
</tr>
<tr>
<td>25-Apr-14 7:13:32 PM</td>
<td>302720F230C746</td>
<td>302720F230C746</td>
</tr>
<tr>
<td>25-Apr-14 7:17:25 PM</td>
<td>302720F230C746</td>
<td>302720F230F8AE</td>
</tr>
<tr>
<td>25-Apr-14 7:21:30 PM</td>
<td>302720F230F8AF</td>
<td></td>
</tr>
</tbody>
</table>
Same location data made meaningful through charting
Eg - Investigator’s PowerPoint to present intercept logs
Eg - Investigator’s PowerPoint to present PGP messages
Eg - Create an Intercept / Data / Event timeline
Questions?