



**DEPARTMENT OF JUSTICE
CANADA
MINISTÈRE DE LA JUSTICE
CANADA**

Lawful Access: Legal Review
Follow-up Consultations: Criminal Code Draft Proposals
February-March 2005

For discussion purposes – Not for further distribution





Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- Preservation Orders
- Other Warrants
- Assistance Orders
- E-mail and other non-oral private communications



Overview

- The purpose of this presentation is to provide details on draft legislative proposals
 - The discussion will be divided into subject matter modules
 - Time has been allotted for each according to perceived interest and difficulty



Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- Preservation Orders
- Other Warrants
- Assistance Orders
- E-mail and other non-oral private communications



Modernizing wording/references

- Interception device: Proposal to bring specificity on the purpose of the device and shorten the current term used throughout the *Criminal Code*
 - “**interception device**” means any apparatus or device, including a computer program within the meaning of subsection 342.1(2), that is used or is capable of being used to intercept a private communication but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;



Modernizing wording/references

- Standardizing reference to telephone, telegraph, cable, etc. to generic term ‘telecommunications’.
- The definition of “telecommunications” would continue to be found in the *Interpretation Act*, but would be repealed in the *Criminal Code*.
- The term “device” would be modified to include ‘a computer program within the meaning of subsection 342.1(2)’.



Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- Preservation Orders
- Assistance Orders
- E-mail and other non-oral private communications



Substantive Offences – ‘Hacking tools’ (s. 342.2)

- Two proposals in relation to the current offence of possessing, distributing, selling, etc. a device under circumstances that give rise to a reasonable inference that the device is used to commit an offence under s. 342.1 (unauthorized use of computer).
 - Add new offences: importing, obtaining for use and making available
 - Directly refer to the mischief provisions under s. 430.
- Would clearly criminalize possession of a virus for the purpose mischief
- Change consistent with Council of Europe *Convention on Cyber-crime*



Substantive Offences – ‘Hacking tools’ proposal (s. 342.2)

- **342.2 (1)** Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or otherwise makes available any instrument or device, including a computer program within the meaning of subsection 342.1(2) or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1 or 430 in relation to data or computer systems within the meaning of subsection 342.1(2), under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,



Substantive Offences – Interception Devices (s. 191)

- Proliferation of “dual-use technologies”
- Existing exemption scheme does not work
- Two possible options:
 - repeal the provision
 - refine the existing provision by allowing for a lawful excuse or justification as in s.342.2 (possessing, etc. of “hacking tools”).



Substantive Offences – Interception devices proposal (s. 191)

- **191.** Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or otherwise makes available any instrument or device, including a computer program within the meaning of subsection 342.1(2) or any component thereof, the design of which renders it primarily useful for the surreptitious interception of private communications, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to section 184, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.



Substantive Offences – False messages (s. 372)

- Proposal to include any form of telecommunication rather than only telephone, radio, etc.
- Currently a summary conviction offence - Propose making the offence hybrid.



Substantive Offences – False messages proposal (s. 372)

372. (1) Every one who, with intent to injure or alarm any person, conveys or causes or procures to be conveyed [by any means] information that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.



Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- Other Warrants
- Preservation Orders
- Assistance Orders
- E-mail and other non-oral private communications



Existing production orders

- Two Production Orders came into force in September 2004
 - General Production Order – similar standard to the section 487 warrant - reasonable grounds to believe – Section 487.012
 - Specific Production Order – Financial and Commercial Information - reasonable grounds to suspect – Section 487.013
- An exemption mechanism was created for Production Orders – Section 487.015 – only available if either
 - Information sought is privileged
 - Unreasonable to require the person to produce the document or data
 - Person does not have the document or data



New Production Orders

- Provisions already exist for tracking warrant and number recorder and telephone records (ss. 492.1 and 492.2).
- Two new production orders would be created:
 - For tracking information – information held by third parties that may assist in locating a person – e.g. where the person last used his debit card.
 - For transmission data – information held by third parties (telcos and ISPs) relating to the traffic data generated by the transmission of a telecommunication – does not included the content of the communication.



Production Order – Tracking Information

A justice, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may order any person

- (a) to produce tracking information or a document — an original or a copy of it certified by affidavit to be a true copy — containing only tracking information; or
- (b) to prepare a document based on the information referred to in paragraph (a) or a document containing tracking information and produce it.



Definition of tracking information

- “tracking information” means information that would assist in determining the location of a person or thing at a particular time.





Production Order – Transmission Data

A justice, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may order any person

- (a) to produce transmission data or a document — an original or a copy of it certified by affidavit to be a true copy — containing information obtained from transmission data; or
- (b) to prepare a document based on data or a document referred to in paragraph (a) and produce it.



New production Orders - Criteria

- The two new production orders would be based on the criteria established in s. 487.013 (Production order – financial and commercial information) with the same judicial safeguards and same information requirements
- Judicial threshold: Reasonable grounds to suspect.





Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- **Other Warrants**
- Preservation Orders
- Assistance Orders
- E-mail and other non-oral private communications



Updates to tracking and DNR warrants

- Proposal to update to take into account new technologies
- Would capture information in relation to which there is a lower expectation of privacy
- Would be issued under the threshold of “reasonable grounds to suspect”
- Valid for 60 days, but could be up to one year if organized crime or terrorism offences



Tracking Warrant – Section 492.1

- Consequential changes to the wording of the tracking warrant provision to be consistent with other changes in the *Criminal Code*.
- Clarifying the scope of tracking tools that law enforcement can use, including items that a person carries that may either be activated or monitored to determine the persons location (e.g. Global Positioning System (GPS) chip in a mobile phone or car, or debit/credit card transactions)



Definition of tracking device

- “tracking device” means any apparatus or device, including a computer program within the meaning of ss. 342.1(2), that may be used to help identify, by electronic or other means, the location of any thing or person.



Transmission Data Recorder – Section 492.2

- Proposal to ensure that the types of call-associated data currently available are made explicit in order to protect the right to a reasonable expectation of privacy
- Need to adapt s. 492.2 to the Internet and allow for the real-time interception of traffic data while excluding private communications
- Definition of transmission data:
 - **“transmission data”** means data relating to the telecommunications functions of dialling, routing, addressing or signalling that identifies or purports to identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility.



Endorsement of Warrants/Orders

- Backing provisions are found in Part VI and Part XV
- Case law has suggested that the endorsement of a warrant/order is an administrative process
- Does not take into account new technologies
- Proposal to remove all requirements for endorsing a warrant or order once issued – effectively allowing the warrant or order to be executed anywhere in Canada



Ancillary Warrants/Orders

- Proposed ancillary warrant/order provision that would give the judge issuing an authorization under Part VI the power to exercise any other powers the judge may exercise under the *Criminal Code* as terms and conditions of the Part VI authorization.



Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offensive
- Production Orders
- Other Warrants
- Preservation Orders
- Assistance Orders
- E-mail and other non-oral private communications



Preservation orders

- Procedural mechanism that allows for the immediate safeguarding of data or documents in the control of the custodian.
- Meant to be a temporary order before search warrant or production order is obtained
 - Council of Europe *Convention on Cyber-crime* suggests 90 days maximum.
- Will require a custodian to save data that they currently have and that is relevant to a specific investigation or proceeding.
- This is a “do-not-delete” order, not data retention.
- Creates a mechanism that does not currently exist to safeguard volatile evidence.
- Could allow for partial disclosure of traffic data necessary for tracing communications, including across borders.



Preservation Order

- (1) A peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, who has reasonable grounds to suspect that a person has possession or control of documents or data that will assist in the investigation of an offence under this or any other Act of Parliament, may, in the course of his or her duties, order the person to preserve the documents or data for a maximum of 15 days.
- An officer could request a third party to preserve evidence (usually computer data) without a judicial order.
- This order would last a maximum of 15 days.



Preservation Order - Notice

- (2) The officer must give written notice to the person that he or she intends to apply to a justice or a judge for a preservation order and that the person may (before the hearing) make written representations concerning the scope, duration and terms and conditions of the preservation order.
- At the time of making the request the officer would notify the third party that they intend to apply for a preservation order and that the third party can make written representations to the justice or judge



Preservation Orders – The Order

- (3) On application by a peace officer or public officer, a justice or a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may order a person to preserve any documents or data referred to in an order made under subsection (1).
- (4) Before making a preservation order, the justice or judge must be satisfied, on the basis of an application containing information on oath in writing and after considering any written representations referred to in subsection (2), that there are reasonable grounds to suspect that
 - (a) the person has possession or control of the documents or data to be covered by the preservation order and that the order will assist in an investigation of an offence under this or any other Act of Parliament; and
 - (b) a warrant or order will be sought to obtain the documents or data.



Preservation Orders – Time Limit

- (6) A preservation order made under subsection (3) is valid for the period mentioned in it not exceeding ninety days from the date that an order was made under subsection (1) in relation to the same documents or data, or if no order was made under that subsection, from the date the preservation order was made. The order ceases to have effect on the day that a warrant or order is issued by a justice or judge to obtain any documents or data covered by it.
- 90 days could be a reasonable amount of time for an officer to prepare an application for and obtain a search warrant or other order from a justice or judge.



Preservation Order – Partial Disclosure

- (5) A peace officer, or a public officer who has been appointed or designated to administer or enforce a federal or provincial law whose duties include the enforcement of this Act or any other Act of Parliament may also order the person to disclose any transmission data in his or her possession or control that is necessary to identify the telecommunications service providers who transmitted the data covered by the order and the transmission route.
- Although the partial disclosure relates to a Preservation Order, the officer's authority to request this information would be found in the Production Order for transmission data.
- This Production Order provision would allow an officer to obtain a sufficient amount of data to determine from which ISP a communication came at the time they request that the service provider preserve data.



Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- Other Warrants
- Preservation Orders
- Assistance Orders
- E-mail and other non-oral private communications



Assistance Orders

- A number of recent court cases have dealt with whether a third party could be reimbursed for expenses incurred in complying with a court order
- In January 2005, the Attorney General of Canada launched an appeal in *Canada (Attorney General) v. Pacific International Securities Inc.*
- In view of this appeal, no proposals on assistance orders will be put forward during these consultations



Agenda

- Overview
- Modernizing wording/references in *Criminal Code*
- Substantive offences
- Production Orders
- Other Warrants
- Preservation Orders
- Assistance Orders
- E-mail and other non-oral private communications



Possible Legal Solution

- 2 possible options based on the following rationale:
 - To reflect social values and the mainstream use of new means of communicating, all private communications should be treated the same, no matter how they are made;
 - The objective reasonable expectation of a party to the communication that the communication will not be intercepted by a third party will continue to dictate the need to obtain a wiretap authorization or not.



Possible legal solution (cont.)

- **Option A**: Treat interception of all private communications alike and employ a new definition of interception or private communication that would make it clear that to intercept a private communication the interception must occur during its transmission. If a private communication is stored anywhere it could be seized under Part XV.
- **Option B**: Consolidate into Part VI all police powers which allow the surreptitious recording and intercepting of one's private activities;
 - This would include bringing the video warrants into Part VI as well as clarifying that the interception of all private communications (oral, e-mail, SMS, instant messaging, etc) fall within Part VI.



Possible legal solution (cont.)

- **Option B** – Interception of private communications:
 - Make it clear that to intercept a private communication, the acquisition must be contemporaneous to the communication being made;
 - Private communications which, because of nature of the technology used, create records (e.g. e-mails and faxes) could be seized after transmission is complete (i.e. not contemporaneously);
 - New definitions for “intercept”, “private communication”, “communication” and “private activity” would be created;



Possible legal solution (cont.)

- **Option B** – Interception of private communications - Possible new definitions:
 - “**private communication**” means any oral communication or any communication by means of telecommunication, that is made under circumstances in which it is reasonable for a party to the communication to expect that it will not be intercepted by any third party;
 - “**intercept**” means the contemporaneous [simultaneous] acquisition of a communication without the knowledge of a party to the communication and includes listening to, or recording, such a communication [or comprehending the substance, meaning or purport of such a communication];
 - “**communication**” includes a conversation or message, whether in the form of speech, data, text or any other form”.
- A definition for “contemporaneous” (or simultaneous) would need to be provided.



Possible legal solution (cont.)

- **Option B**: Making a visual recording
 - The general warrant provision under s.487.01 would be amended to remove references to video surveillance;
 - The existing provisions of Part VI would be amended and adapted to allow for video surveillance authorizations where appropriate;
 - A new offence for making a visual recording could be created:
 - “Every one who makes a visual recording of a private activity, maliciously or for gain and without the knowledge of the person carrying out the activity, is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years”.
 - A definition for “private activity” would be provided for:
 - “**private activity**” means any activity that is carried out in circumstances in which there exist a reasonable expectation of privacy for a person in regard of his or her movements or image”.



Amendments to other federal laws

- *Mutual Legal Assistance in Criminal Matters Act*
 - Amendments to allow for the ratification of the *Council of Europe Convention on Cyber-crime*.
- *Competition Act* amendments



Questions?

For more information:

Summary report and consultation paper available at:

http://www.canada.justice.gc.ca/en/cons/la_al/