



BC FREEDOM OF
INFORMATION
AND PRIVACY
ASSOCIATION

Comments on New Lawful Access Proposals (March 2005)

**FIPA submission to a consultation
conducted by Justice Canada**

April 29, 2005

BC Freedom of Information and Privacy Association
103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148
Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

FIPA wishes to acknowledge the Law Foundation of British Columbia for their ongoing support of FIPA's activities in the areas of law reform, research and public education



BC Freedom of Information and Privacy Association

103 - 1093 West Broadway, Vancouver, BC V6H 1E2

Ph: 604-739-9788 • Fax: 604-739-9148

Email: fipa@vcn.bc.ca • Web: www.fipa.bc.ca



April 29, 2005

Christopher Blain
Criminal Law Policy Section
Justice Canada
East Memorial Building, Room 5016
284 Wellington Street
Ottawa, ON K1A 0H8

Dear Sirs/Mesdames:

Comments on the Lawful Access Proposals (March 2005)

In 2002, the B.C. Freedom of Information and Privacy Association (“FIPA”) co-hosted a consultation session in Vancouver on the Lawful Access Consultation Document (“Consultation Document”) with Justice Canada, and made submissions to the federal government. Subsequently, in March 2005, FIPA co-hosted a follow-up consultation concerning further Lawful Access Proposals (“New Lawful Access Proposals”).

FIPA welcomes the opportunity to comment on these new proposals. This submission should be read in conjunction with our previous submission of December 16, 2002, which is attached.

In summary, FIPA continues to be opposed to many of the New Lawful Access Proposals as they unjustifiably intrude upon the privacy rights of Canadian citizens. We repeat the concerns outlined in our letter of December 16, 2002. Our further concerns arising specifically out of the New Lawful Access Proposals are set out below.

Summary of Concerns

In both the Consultation Document and the New Lawful Access Proposals, the federal government states that the purpose of the proposals is to be able to effectively and efficiently maintain lawful access to electronic communications for crimes relating to or assisted by new technology. This need must be balanced against citizens’ rights to privacy and freedom from unreasonable search and seizure. In our view, the proposals do not adequately address that balance.

Here are the concerns we have with the New Lawful Access Proposals:

1. The proposals do not merely maintain, but significantly enhance the ability of law enforcement agencies to intrude into the privacy rights of Canadian citizens.
2. Some proposals such as preservation orders are not limited to the stated concern of electronic documents or communications, but apply to all documents and data.
3. There continues to be a lack of empirical or any evidence that would justify these enhanced powers, or that would enable citizens to weigh whether the enhanced powers are justified.
4. The proposals fail to adequately recognize the intrusive quality of electronic surveillance and the sensitive nature of information that can be obtained from electronic communications and data, and the correspondingly high expectation of privacy associated with them. The proposed lower thresholds for legal access to electronic data and communications are not appropriate.
5. There is a lack of any judicial or other adequate oversight for some of the proposals.

Technical Infrastructure and Intercept Capability

The federal government again has not provided empirical or other data to substantiate the difficulties it has encountered that, with limited exceptions, would justify mandated intercept capability across all telecommunications service providers. Without this evidence it is impossible to determine whether the costs and risks of such a potent privacy-eroding proposal are proportionate to the benefits.

We continue to have concerns with respect to the effect of this proposal on universities, colleges and public libraries. These facilities have traditionally been available to the public for anonymous research and communications. Many libraries have Internet workstations that do not require IDs and passwords. It is now proposed that post-secondary educational institutions and libraries would be obligated to provide an authorized person (i.e. with a warrant) information on the telecommunications services and features that it provides to a person who is the subject of an interception. This would effectively prevent any anonymous communications or research using technology. There is no evidence presented that would demonstrate how the effect of this proposal, a serious erosion of privacy rights, would be effective in the fight against crimes assisted by new technology.

The federal government proposes that Telecommunication Service Providers (TSPs) be required to have the capability to isolate the transmission data of the person whose telecommunications are authorized to be intercepted from his or

her telecommunications (content), and to provide that information to authorized persons. The proposal places on the TSP the burden of deciding what is content and what transmission data. It raises significant concerns that privacy will be violated if content is inadvertently or improperly disclosed. TSPs, who are in the business of providing transmission services and not surveillance, should not be turned into agents of law enforcement officials.

The proposal creates a latent surveillance system. Mandating intercept capability may result in telecommunications systems being more vulnerable to being used by criminals to perpetrate crimes or being used to breach citizens' privacy. We must ensure that there are appropriate security measures in place so that the proposal does not have the unintended consequence of decreasing security, and hence decreasing trust, in telecommunication systems.

Finally, we must ensure that access capability (technical ability) does not lead to a lower standard for lawful access (legal inevitability). Legal access must only be granted through judicial warrant when appropriate thresholds are met, taking into account the reasonable expectations of privacy in the information sought.

Production Orders, Updates to Tracking and Dial Number Recorder (DNR) Warrants, and Subscriber Information Proposals

In the 2002 Consultation Document, the federal government proposed the enactment of:

1. a general production order (threshold: reasonable grounds to believe);
2. a specific production order for transmission data (threshold: reasonable grounds to suspect); and
3. a specific production order for subscriber information (no threshold specified, but low threshold implied); or creation of a national database of subscriber information.

Since that time, the general production order has been enacted (*Criminal Code* s. 487.012). In addition a specific production order for limited financial information has been enacted. In the New Lawful Access Proposals, the federal government proposes:

1. a specific production order for transmission data as previously proposed; but also
2. a specific production order for tracking information (threshold: reasonable grounds to suspect)
3. expansion of the current DNR provision (*Criminal Code* s. 492.2); and
4. expansion of the current tracking warrant provision (s. 492.1); and
5. that subscriber information no longer be provided by order, as previously proposed, but on the "written or oral request" of a "designated person".

There is no threshold requirement. The alternate proposal of a national database has been abandoned.

(i) Production orders for transmission data and tracking information

Currently, the production of traffic data and tracking information may be ordered under the general production order provision (reasonable grounds to believe). The New Lawful Access Proposals call for a carving out of traffic data and transmission data from these provisions, and for the threshold for production of this data to be at a new lower standard (reasonable grounds to suspect). These proposals would effectively circumvent the higher threshold currently required, and are an erosion of privacy rights.

The rationale provided for the lower standard is the alleged lower expectation of privacy in traffic and transmission data. We fundamentally disagree with this and repeat our submissions of December 2002, that there is not a lower expectation of privacy in this information.

Technology is pervasive and constantly evolving so that an increasing amount of personal information is available to be collected, aggregated, and analyzed. Post-call cut-through digits are one example of how information obtainable from dial number recorders has expanded with the development of technology. A tapestry of information is available from transmission data and traffic information. It is not appropriate to permit access to transmission data and traffic data at a low threshold.

Any analogy of transmission data or traffic data to data obtainable under the current DNR warrant, or the new specific production order with respect to financial information, or the current tracking warrant, is false.

Transmission data is not the new technology equivalent to DNR information; it is qualitatively and quantitatively different. Transmission data with respect to Internet use especially, provides insight into the thought process, associations, and interests of a person. It is a private activity that is akin to video surveillance or interception of private communications where a high threshold for legal access is mandated.

Similarly, transmission data is not akin to information obtainable under the new specific production order for financial information. The information available under this provision is limited, being only the account number, the status and type of the account, the name under which the account is registered, and the date on which the account was opened or closed.

Traffic data is not similar to information that can be obtained through an installed tracking device. A tracking device on a vehicle will tell the police agency that a vehicle is at the intersection of two roads. Use of a GPS

system on a cell phone, or use of a credit card at a certain store at that intersection, will give more information.

Finally, it will be difficult if not impossible to separate content from strict address information. Attempts to define transmission data are not helpful as some transmission data, however defined, will contain or imply content. The federal government's proposal of filtering raises many questions as to its effectiveness.

The entire debate and issues surrounding what is content and how to separate it from strictly addressing or location information can be avoided by recognizing the reasonable expectation of privacy that Canadian citizens' have in this information, and protecting all of it at an appropriate high threshold for legal access.

(ii) Expansion of current provisions for DNR and tracking warrants

The federal government proposes that the definition of tracking device in s. 492.1 be expanded to include a computer program. The device need no longer be installed. The government states that this proposal will clarify the scope of tracking tools that law enforcement can use. It is an expansion of the tools. Under this new proposal, features of many private devices and services could be used to track an individual's location – e.g. activation or monitoring of the GPS system on cell phones, the use of credit and debit cards.

We repeat our comments above, that the information available from this type of technology is qualitatively and quantitatively different from that which was previously available under more conventional tracking devices, and a lower threshold for obtaining this information is not appropriate.

Similarly, the federal government proposes that the DNR provision in s. 492.2 be expanded to include the real-time interception of transmission data. Again, we repeat our previous comments that this information is not similar to DNR data and a low threshold of reasonable grounds to suspect for legal access is not appropriate.

(iii) Subscriber information and other identifying information

In the Consultation Document, the federal government proposed that subscriber information could be produced by order. No threshold was specified but a low threshold was implied. Alternately, the government raised the suggestion of a national database. This latter suggestion now appears to have been abandoned.

In the New Lawful Access Proposals, the federal government proposes that subscriber information now be available not on an order, but “on written or oral request” of a “designated person”. A TSP would be required to produce any information in its possession or control respecting the name, address and prescribed identifiers of any subscriber to its telecommunications service. There is no threshold mandated.

This is in effect a warrant-less search of citizens’ personal information. It is not tied to any alleged offences. There is a lack of any judicial authorization or legal threshold that would serve as a check to ensure there is no unjustified access to this private information. In addition, there appears to be no adequate oversight of the “designated persons”.

The federal government suggests that this will not mandate collection or retention of subscriber information, but these proposals will create the pressure to do so. In the end there is the risk that a national database will be constructed, except that it would be held by TSPs instead of the government.

The creation, in effect, of a national data base available to law enforcement agencies without adequate oversight or thresholds is very worrisome. The aggregation of vast quantities of data, and the ability to link these with a national data base of subscribers could lead to a significant erosion of privacy rights in Canada.

Finally, there is again a lack of evidence that law enforcement agencies are having difficulty in obtaining this information in appropriate situations, and that would justify these proposals.

Preservation Orders

In the Consultation Document, the federal government proposed “an expedited judicial order” that would require service providers to save existing specific data. It also proposed that in exigent circumstances, law enforcement agencies should be able to impose a preservation requirement on a service provider without a judicial order for a specified period such as four days.

In the New Lawful Access Proposals, the federal government proposes that law enforcement agencies be able to “order” a “person to preserve documents or data for a maximum of 15 days”. During those 15 days, the law enforcement agent would apply to obtain a judicial preservation order on the threshold of “reasonable grounds to suspect”. This judicial order could provide for preservation up to 90 days in total. The proposal in the Consultation Document that this be done only in exigent circumstances has been abandoned, and now the reverse order of securing preservation is implied – that law enforcement agencies make an order without judicial authority in effect for up to 15 days, and then apply for a judicial preservation order.

This proposal is an unprecedented and significant expansion of police powers. The rationale for these proposals is the volatile nature of electronic evidence. However, no attempt has been made to limit the scope of these provisions to electronic data or situations where data is in danger of being destroyed, or to exigent circumstances.

Finally, the federal government proposes a partial disclosure without warrant to identify the TSP's who transmitted certain data. It is unclear how the partial disclosure provisions of the preservation order would be implemented. In order to make a request to determine from which TSP a communication came, a law enforcement agent would need to be informed of what communications there were. This would effectively be a search without warrant. If preservation orders are enacted, it must be mandated that disclosure is prohibited until judicial authorization is obtained.

Again, no empirical evidence has been given to demonstrate how and when law enforcement agencies are being thwarted by destroyed electronic or paper data or documents.

E-mail

Whether e-mail should be treated as a private communication and only accessed under Part VI (interception), or treated as a document and accessed under Part XV (search and seizure) continues to be an issue. As stated in our December 2002 submission, there is a high expectation of privacy in e-mail and lawful access to it should be obtained only under the high standard for interception. The expectation of this privacy does not change because the e-mail is in transit one moment, and stored on a server the next.

We repeat our previous submission that the federal government must provide a well-argued system of privacy protection for private communications, where the particular form of the communication used is not determinative of the protection provided. It is the reasonable expectation of privacy, and not the form of the communication (which changes as technology develops) that should dictate the threshold required for legal access.

Summary

We recognize the need to be able to effectively and efficiently combat crimes that are enabled or assisted by new technology, but lawmakers must ensure that in doing so we do not unnecessarily and unjustifiably intrude upon the privacy rights of Canadian citizens. Lawful access proposals must be shown to be truly required, reasonable, demonstrably justified, effective and proportionate to the ends to be achieved. Many of the New Lawful Access Proposals do not meet those requirements.

We would like to thank you for affording us the opportunity of meeting with government representatives in Vancouver and of providing further submissions on these important proposals.

Yours sincerely,

Darrell Evans
Executive Director
BC Freedom of Information and Privacy Association