FIPA

BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

Consultations on Lawful Access: Meeting with Civil Society Groups in Vancouver, March 15, 2005

Report of Proceedings

BC Freedom of Information and Privacy Association

August 25, 2005

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

Table of Contents

Department of Justice Consultations on Lawful Access: Meeting with Civil Society Groups in Vancouver March 15, 2005

Rapporteurs: Prof. Richard S. Rosenberg, Professor Emeritus, Dept. of Computer Science, University of British Columbia
Barbara Norell, Barrister & Solicitor, Harper Grey Easton

Background

On August 25, 2002, the Department of Justice, Industry Canada, and the Solicitor General of Canada released the Lawful Access Consultation Document and solicited comments on "matters relating to amendments to the Criminal Code and the Competition Act to permit lawful access to certain kinds of information."

Meetings were held in Ottawa, Montreal, and Vancouver in October and November, 2002 with a variety of representatives of Civil Society Groups. Other meetings with interested parties were also held. The call for submissions resulted in responses from "law enforcement, companies, organizations and the public in response to the proposals presented in the consultation document." Some 219 individuals responded, almost all Canadian, as well as 19 companies from relevant industries, 14 civil society groups, five privacy and information commissioners and the Canadian Association of Chiefs of Police. A Summary of Submissions was made available on August 6, 2003. Interestingly, none of the submissions were made available on the Department of Justice website.

It should be useful to include here a summary of views expressed by Civil Society Groups during the first round of consultations, in order to compare it with views and comments expressed during the Vancouver meeting in 2005. In 2002, the summary of views was that:

1. The consultation document is unclear about the government of Canada's proposals.

2. The draft legislation and accompanying regulations should be made available for full and complete public review with sufficient time for interested parties to assess their impact and submit comments.

3. The document is unconvincing on how the proposals would actually help fight organized crime or terrorism. The government will no doubt have more access to the private lives of Canadians, but serious criminals and terrorists are unlikely to be careless enough to fall within the scope of the proposed measures.

4. If evidence is available to justify the proposed legislative amendments, it should be made public so that it can be seen whether the security benefits outweigh the privacy costs. If such evidence does not exist, the measures should be dropped.

5. The proposals would establish a lower standard for lawful interception and/or search and seizure of online communications versus telephone and postal mail, for example. No justification has been provided for this. *Criminal Code* standards should be designed to apply regardless of technology.

6. Any new legislation should specifically address privacy issues wherever individual privacy is at risk. General references to the *Canadian Charter of Rights and Freedoms* (the *Charter*) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) are insufficient.

7. The government has failed to present evidence that this massive surveillance infrastructure is necessary. For example, it is unknown how many investigations have actually been seriously hampered by lack of technical capability.

8. If law enforcement agencies have difficulty in dealing with new communications technologies, the solution is not to lower legal standards for interception, but to provide law enforcement agencies with the technical expertise and equipment they need to deal with the evolving environment.

9. The proposals require customers or their ISPs to pay for the surveillance. This is wrong in principle and impracticable in operation.

10. The job of ISPs is to provide services for their customers. This should not include monitoring those customers for the purposes of the state. Production orders must not be used to circumvent the high thresholds that would be required if law enforcement agencies were carrying out the search or interception themselves.

A last point worth noting is that after August 6, 2003, the Department of Justice made no contact with the public about Lawful Access issues until February 2005, when it contacted civil society groups in order to organize follow-up consultation sessions in March 2005. From the agenda distributed by the Department of Justice on behalf of the federal departments at the Vancouver session, the purpose of the follow-up meetings was as follows:

- To present more details about Criminal Code Draft proposals,
- To present proposed amendments to the Competition Act,
- To present proposals with respect to compelling interception capability and access to subscriber information,
- To provide an opportunity for civil society experts to discuss and respond to these proposals,
- To facilitate an open discussion.

LAWFUL ACCESS CONSULTATION
FOLLOW-UP MEETING WITH CIVIL SOCIETY GROUPS

Presented by
Justice Canada
BC Freedom of Information and Privacy Association

DATE: Tuesday, March 15, 2005
TIME: 9:00 am - 4:00 pm
LOCATION: Salon 1, The Westin Bayshore
1601 Bayshore Drive

AGENDA

8:30 – 8:45	Welcome
8:45 – 9:15	Overview
9:15 – 10:00	Criminal Code Draft Proposals
10:00 – 10:15	Break
10:15 – 12:15	Criminal Code Draft Proposals (continued)
12:15 – 1:15	Lunch break (lunch will be provided)
1:15 – 2:15	Proposed Amendments to the Competition Act
2:15 – 3:30	Proposals with Respect to Compelling Interception Capability and Access to Subscriber Information
3:30 – 3:45	Break
3:45 – 4:45	Response Panel
4:45 – 5:00	Wrap-Up

Summary of Key Comments

No one in the group assembled for the Vancouver consultation questioned the need for lawful access provisions in the Criminal Code and the Competition Act to address new technologies. However, there was substantial opposition to many of the proposals, and the following summarizes the key recurring comments made throughout the consultation:

The proposals went beyond what was required by the Council of Europe Convention on Cyber-crime.

The proposal of a lower threshold for obtaining legal access to transmission data was not acceptable and a higher threshold should be mandated. The analogy put forth by the government that transmission data is akin to DNR data, and that it does not attract a higher reasonable expectation of privacy, is false.

It will be very difficult to isolate certain traffic data (e.g. header information) from content, as suggested by the federal government.

E-mail, whether in storage or in transit should be protected at the higher threshold.

As in the 2002 consultation, there is a lack of empirical evidence to prove what difficulties, if any, the federal government is encountering with the current lawful access provisions and which would justify some of the proposals.

The March 31, 2005 deadline for submissions does not provide enough time for adequate consultation and preparation of submissions. The deadline should be extended.

Summary of Presentation

Introduction

The day began with welcoming remarks from co-hosts Christopher Blain of Justice Canada and Darrell Evans of B.C. Freedom of Information & Privacy Association.
Norman Wong of Justice Canada followed with a presentation based on the PowerPoint document, **"Combating Cyber-Crime: The Context"** (D)[1]. (It should be noted that a hard copy of D was not made available to the participants until about 10 days after the Vancouver meeting.)

This presentation stressed benefits of the Internet, for example, Government on-line service for all Canadians; e-commerce, e-learning, e-medicine, e-banking, etc. However, criminal activity, including viruses, trojans, worms, etc., phishing, ID theft, Internet fraud, and money laundering have flourished. Trends (taken from the 2004 CSI/FBI Computer Crime and Security Survey Thus identity theft is the fastest growing crime in the U.S. Given that Internet-based crime is growing rapidly, law enforcement requires expanded powers. The argument is that lawful access powers must be extended to the Internet and the Criminal Code updated appropriately. A balance needs to be achieved among sovereignty, security, privacy, human rights, and e-commerce and solutions to fighting cyber-crime in the New Reality.

Lawful Access (Document A)

New legislation will require modernizing wording/references, such as the definition of "interception device" in particular to bring specificity on the purpose of the device and shorten current term used throughout the *Criminal Code*; standardizing reference to telephone, telegraph, cable, etc. to generic term 'telecommunications'. The term "device" would be modified to include 'a computer program within the meaning of subsection 342.1(2)'. A number of Sections could be affected, including those dealing with interceptions of communications, unauthorized use of computer, false messages, and mail fraud. In a change consistent with the Council of Europe *Convention on Cyber-crime*, new offences are proposed for: importing, obtaining for use and making available devices that give rise to a reasonable inference that the device is used to commit an offence under s. 342.1. 342.2 is a substantive offence – 'hacking tools' proposal. Another substantive offence is the interception devices proposal (s 191). It is important to refine the existing provision by allowing for a lawful excuse or justification as in s. 342.2 to permit private use of software and devices that can trap offensive software. The false messages proposal (s. 372) provides an indictable offense for every one who, with the intent to injure or alarm any person, conveys or causes or procures information that he knows is false

Production Orders

As a prelude to proposals for new production orders, existing production orders were reviewed. Two production orders came into force in September 2004: General production order –similar standard to the section 487 warrant – reasonable grounds to believe and

[1] Briefing documents provided by government are coded as A through G. See Bibliography, page 22.

Specific production order – financial and commercial information –reasonable grounds to suspect. An exemption mechanism was created (s. 487.015) if the information sought is privileged, etc. Two new production orders would be created: for tracking information, i.e., information held by 3rd parties that may assist in locating a person –e.g. where the person last used his debit card.; for transmission data – information held by 3rd parties (telcos and ISPs) relating to the traffic data generated by the transmission of a telecommunication – does not include[d] the content of the information [emphasis added]. A series of questions and answers followed.

To enlarge the scope, government seems to want the same type of information in the Internet world as that available in the telephone world, i.e. traffic data on the Internet and dialing information for the telephone. Which one for locating a cell phone? The answer is tracking information. .A justice, a judge of a superior court …may order any person (a) to produce tracking information … or (b) to prepare a document based on information referred to in paragraph (a) … and produce it. "Tracking information" means information that would assist in determining the location of a person or thing at a particular time. "Transmission data" means data relating to the telecommunications functions of dialing, routing, addressing or signaling 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.

The identity of the individual is the central piece of information and this opens up many issues. Isn't this so? A justice, …, may order any person (a) to produce transmission data … or (b) to prepare a document … What about the protection of journalistic sources? Probably, protection would not apply to journalistic sources. (Note, this response is limited and may possibly be inaccurate.)

Combating Cyber-Crime

This presentation of issues related to Criminal Code Draft Proposals was continued after the break. The presentation by Gareth Sansom, connected via a telephone link from Ottawa, was based on document D. The main challenges to defining transmission data are the following:

- must address contemporary telephony but must extend to also deal with Internet "traffic data" but avoid the pitfalls that threaten "technology-neutral language;"
- in constructing definition, some individuals have argued that such data "should not include the contents of any communication;"
- at a practical level, there are circumstances ("header information" in some packets; post-call cut through digits in telephony) where content is apparently not excluded

In general, "content" is not a helpful term.

The notion of "reasonable expectation of privacy" places a great burden on the individual to determine an ordering on various means of communication prior to employing a particular one. Such a burden makes little sense as the number and variety of communications methods continues to grow. How can such a problem be dealt with? Reference was made to document A, slide 21.New production orders (financial and commercial information), would be based on the criteria established in s. 487.013. to take into account new technologies. This would capture information in relation to which there is

a lower expectation of privacy (emphasis added). Orders would be issued under threshold of "reasonable grounds to suspect," valid for 60 days but could be up to one year if organized crime or terrorism offences are implicated

How is it possible to distinguish between header and content information? So for example, a URL could contain www.safesex.com, which provides much more information than a called number for telephone communication. There was a great deal of skepticism expressed about the ability to distinguish these two. When ISPs hand over information to a peace officer, do they filter out information with an "expectation of privacy"? It would be helpful to have an overall view of government's intentions rather than nitty-gritty details. Who, when, how are not as clear as what, you say? If I have done nothing wrong, then I have a right of privacy including anonymity but you seem to be expressing a view that you still have a right to get the information because the new technology makes this possible. What about the use of encryption? What about reasonable expectation of privacy awareness by individuals? Some issues you raise are currently before the courts but it is important to note there is not much precedent on many of these matters.

What determines how hard or easy it is for police to obtain a warrant, with respect to tapping? The basic concerns depend on evolving notions of privacy. It is difficult to discuss issues of privacy in the abstract, especially with respect to the Internet, etc. Suppose a call comes in that a neighbour is a pedophile, can police obtain a warrant? They cannot obtain a court order based on an anonymous call.

E-mails and Criminal Law Policy (document G)

Email communications are analogous to both telephone communications and letters but email can be acquired at several locations, e.g. during input at keyboard, while transmission is stored on sender's computer, during transmission at several points along the way, including when it is either at the sender or recipient's ISP? Voice and text have differences and similarities. Over a network, the raw material is similar, digitized communication. The basic question is: Do voice and text communications attract the same reasonable expectation of privacy? The current Criminal Code definition of "private communication" includes the notion of reasonable expectation of privacy. There is an argument for an equivalent status for email as well as a counter-argument for the opposite. Three hypothetical scenarios for intercepting email are presented, as follows:

1. Interception by personnel accessing mail servers. Note also that this is straightforward for personnel in telephone companies.
2. Interception in a large corporation. Except for IT personnel, is it possible for anyone in a corporation to intercept other's e-mail? Existence of packet-sniffers does mean anyone can use them.
3. Intercepting your neighbour. Is it easy for average Canadians to intercept their neighbours' email? Even if answer is yes, this situation should not diminish the expectation of privacy.

Who bears costs of preservation orders? How much of a financial burden is there? A case pertaining to Assistance Orders was before the courts at the time of this consultation and so the government did not wish to comment on these particular orders. However, the government was willing to talk about production orders.

Lawful Access – Amendments to the Competition Act (document B)

Questions and answers resulting from this presentation were to provide examples under which the MLACMA would be used to which the government replied with, "a case for a 'vitamin' cartel." Concern was also expressed about how requests from the FBI would be dealt with. In competition and anti-trust matters, the Commissioner is competent to apply for warrants in Canada on behalf of U.S. officers. The threshold is the same as for search warrants. Does Canada intend to ratify the Council of Europe's Cybercrime Convention? The answer was yes.

Lawful access consists of lawful interception of telecommunications and search and seizure of information. Authorities consist of the Criminal Code and the *Canadian Security Intelligence Service Act* (CSIS). Oversight and accountability derive from the Charter, Privacy Legislation, the courts, annual reporting to Parliament, etc. The policy objectives of the proposals is clearly stated as lawful access is **not** used to monitor everyone's telephone and Internet communications and nothing being proposed will change that. All interceptions will continue to require lawful authorization. [emphasis added] Another policy objective is to minimize costs to industry and governments. However, when TSPs for business reasons buy new equipment, they would also be required to bear some additional costs for public safety. These proposed obligations would be consistent with international technical requirements in U.S., U.K., and Australia. A series of questions followed. The proposal to compel companies to incorporate interception capabilities as part of the design process places a financial burden on them; why should they bear these costs? The government's response is that consultations are ongoing as to how companies will be impacted. The public sector needs to pay, c.f., the car industry installing safety belts and pollution controls.

Some are concerned that technological capabilities are driving the need for lawful access interception abilities. For the government, laws are laws! The only new issue is building in capability. Consultations are necessary to assure that companies, which have been in discussions with government over many years, will continue that dialogue. Why require companies to bear costs? Again the argument is that retrofitting is much more expensive than building in capability, *ab initio*. But again why should new technology be required before the proposed law is seen to be constitutional? We (the government) have authorization to do this so that when courts give OK, companies are ready to go at reasonable costs. But it is a qualitative change in Canada's communication system to convert it in part into a surveillance system. The goal is to put in place legislative requirements. But what will be done about diversity, size, and possible unfairness of the requirements? Yes, these could be and must be monitored.

Small TSPs (under 100,000 subscribers) would be exempt from some requirements deemed too costly. [So these TSPs would not be subject to certain production orders] TSPs who provide telecommunications services ancillary to their principal function of operating

a post-secondary educational institution, library, community centre, restaurant, hotel, apartment building, or condominium [emphasis added] would have partial exemptions, i.e., only certain limited obligations for these entities. Note, an authorized person (i.e. with a warrant) could bring equipment to carry out an intercept. There was an interest in seeing a specific list of community networks, telecentres, etc. and a question about the status of religious institutions. Finally, subscriber and TSP will be subsidizing costs of their own surveillance; so this a major shift in how we conduct surveillance in our country, i.e. a new thing not just tinkering.

TSPs would be required to remove any encoding, compression, encryption or any other treatment of intercepted information. But what if information is encrypted by sender? Police already have legal rights to obtain this information; so what do TSPs need to provide technically? Answers are provided in Document C, for example, infrastructure obligations as re location of equipment that is subject to an interception. So the government proposal is to mandate that all cell phones implement tracking, i.e. GPS abilities. Under emergency orders, Minister could pay TSP to comply. Every TSP that is providing telecommunications services would be required to submit a report to the Minister within six months after proposals come into effect. Why are there differences in partial and full exemption? It is because of historical evidence of where needs have been required. But what differentiates the two lists? No evidence is supplied about how distinctions are made. For example, for hotels it is most likely that drug dealers will go there to do business but no evidence of the similar use of houses of worship. What is the hard evidence on which these distinctions are based? If the intent is to provide actual numbers, then, no these cannot be provided.

Every TSP would be required to provide to designated persons, … name, address, and prescribed identifiers of any subscriber to its telecommunication service. [It does not include content, for which a search warrant would be necessary.] There is a need to clarify authority to receive information. Apparently, government officials have consulted with PIPEDA experts at Justice as well as other privacy experts. Safeguards include a limited number of people who can request or have access. Finally, proposal will not require or mandate the collection of subscriber information. Designated persons are defined, how the information is to be retained is described, and other safeguards are described as well. This proposal codifies current practices; the retention of records is necessary for oversight purposes. These place restrictions on TSPs. Information must be supplied in at most 72 hours but immediate response must be no longer than 30 minutes. Of course, it may be difficult for small TSPs with limited staff to respond this quickly.

One attendee was astonished that this activity was going on now without any lawful permission and in the violation of privacy laws. All this seems to be an argument for a database of information, of which various pieces have been produced by a designated person, not necessarily a police officer. A concern was expressed with an agency [?] for monitoring and oversight of police, etc. Intrusion into one' privacy and even anonymity is incongruous. What about Canadian individual information held outside Canada? What about information being sent back without original oversight to Canadian officials?

Response Panel: Concluding Comments

Following the government presentations and the question and answers made throughout the day, a response panel assembled by FIPA made some brief comments:

Dan Burnett
Barrister & Solicitor, Owen Bird

If these new production orders are something akin to a warrant, what is the justification for a lower threshold? The standards proposed are lower – "suspect", not "believe", and I am concerned about this relaxing of standards. The justification is not there. The internet creates a more permanent record than the telephone. Warrants and intercepts are difficult to obtain for good reason.

I am concerned we are building a latent surveillance system. Criminals will just avoid the more highly surveilled media – e.g. communicate during a walk in the park. Tools are already in existence for police so long as they are technologically provided for. What's next – will every new home that gets built have to have a hidden video and microphone?

Micheal Vonn
Policy Director, B.C. Civil Liberties Association

I am concerned about the tone of what we heard today regarding what is a "reasonable expectation of privacy". I read case law today very differently from the way government officials read it. It is shocking to hear that certain communications do not have a reasonable expectation of privacy.

In R. v. Plant, the Supreme Court of Canada said that the case was very close to the line. The court reviewed factors such as the nature of the information, the relationship between the parties, the place, the manner and the seriousness of the crime. The required analysis of the expectation of privacy is much richer than the government says.

I also wish to state that we are being given an outrageously short of amount of time to respond to these proposals.

Aziz Khaki
Committee for Racial Justice

The consultation process has meaning to me to demystify the process of lawful access. Probably most things are already decided. Today I heard that the police already have the power to do certain things, but these powers are subject to restrictions and regulation. However, most regulations do not respect the spirit of the legislation. Regulations do not go to Parliament. There is a problem in defining terrorism and how much we bow to international pressure in creating laws. How much do we actually protect our citizens under the Charter?

Brian Campbell
Founding Chair, Canadian Library Association Information Policy Committee
Founding President, Vancouver Regional FreeNet Association

We don't have a big picture justification for these proposed changes. This is just another part of a surveillance regime and Anti-terrorism legislation. I don't think the consultation serves the process, given the time line for submissions, which is so short that it must make us question the government's sincerity.

There is no empirical evidence to justify these proposals. There are a number of contradictions – for example, to remove encryption and to exempt certain TSP's. Where do we think the bad guys are going to go? The customer name and address proposals in particular are shocking. There is no attempt to limit them to severe circumstances, and there is no limit to the use of the information.

I am concerned about the cooperation between industry and government. The proposal to use filtering to get only certain information is highly suspect. The comparison of the telephone as an analogy to the internet is not correct; these are not comparable. We didn't get into the question of cybercrime and how Canada stands on international initiatives – what are the external influences and pressures we are buying into.

Some of the proposals have been improved since 2002, such as the e-mail proposals. The fact remains that these proposals represent the thin edge of the wedge in eroding privacy rights. Expanding to the rest is an easy shift of attitude. We haven't really dealt with the need to protect the reasonable expectation of privacy.

Michael Lucas
Staff Lawyer, Policy and Legal Services
Law Society of British Columbia

The powers proposed are not limited to electronic communications. We haven't heard any justification why they are not limited to offences involving computers. Why do we need broader powers for old types of offences? Why shouldn't you limit these powers to computers and electronic communications?

Overview of Issues of Concern

Criminal Code Proposals

(i) Substantive offences

Very little comment was presented.

(ii) Transmission data, Production Orders and Tracking and DNR Warrants

Considerable discussion took place. The lower threshold of "reasonable grounds to suspect" is not appropriate and a higher threshold should be mandated. Tracking information and transmission data does not attract a lower expectation of privacy as suggested by the government. Data that falls within the proposed definition of transmission data (eg. URL addressing data) does give information that attracts a reasonable expectation of privacy (e.g. URL with "same sex marriage"). The existing lower threshold for financial production orders (s. 487.013 – financial and commercial information – which gives very limited information) is not analogous to transmission data. The proposals are the thin edge of the wedge toward a breakdown of private communications into private and non-private components.

Even tracking information intrudes on privacy - an example of "information gallop". Citizens have a right to anonymity unless they have broken the law, and a threshold of "suspicion" is too low. How will citizens know what level of privacy they have? Level of privacy should not depend on the form of communication. The proposals do not deal with encryption (confirmed by government). All criminals will encrypt communications and be beyond the reach of the law. The result is that only those innocent citizens who do not encrypt will be subject to having their communications accessed at the low threshold of "suspicion". What is the difference between "suspect" and "believe" in the two thresholds?

It is very difficult to distinguish between traffic data (for example headers) and content that is protected. The federal government suggests that filtering is a possible solution. Concern was expressed with respect to where the filtering would occur (government answer: 1. legal definition of transmission data, and 2. at service provider within infrastructure). Concern was expressed that an ISP will not know what to filter (e.g. solicitor-client communications or journalistic sources). Concern was also expressed with respect to what remedy there would be for inappropriate filtering? (No answer was given). The proposed production orders may allow searches that would intrude on solicitor-client privilege. Also, the proposal to remove requirements for endorsing a warrant or order from another province causes concern in B.C. where there is a practice direction regarding law office searches that may result in a higher standard than other provinces. A note was made that the CRTC is currently considering 911 GPS capability for internet telephony.

(iii) Preservation Orders

Considerable discussion ensued. Concern was expressed that preservation orders go well beyond lawful access, and represent a significant enhancement of police powers. The proposals are not limited to electronic data, but could be used to preserve all data including paper documents. (Government answered that this was not the intent). Who is included in the description of "a public officer who has been appointed or designated to administer or enforce any federal or provincial law"? What authority do the police have to "order" a person to do something? (Government answered that the French version of the proposal is clearer). Comment: Citizens should not have to read the French and English versions of the Code to understand what the provision means.

Would schools and public libraries be subject to these orders? What happens to information that is saved but not seized? What training is there for people who are custodians of preserved data? In the 2002 consultation it appeared that the proposal for preservation orders would include future information. The government clarified that the current proposal is that preservation orders would apply to past and present data only, and that DNR orders would apply to future data. How does this impact the CRTC's "Subscribers Bill of Rights"?

Why is there only provision for written representations? Could a party make oral submissions? (Government answers that the application is made ex parte and the person could apply for certiorari.) If the objective of the provision is to protect volatile information that is in danger of imminent destruction, then why not limit the preservation order to exigent circumstances such as already exist in the Code? What provision is there to deal with a lawyer's professional obligation to notify his/her client of a preservation order? (Government answers that the judge will set terms and conditions.)

Ninety days seems like a long time to get a warrant. Why is the preservation order in effect for so long? (Government answers that most warrants do not require that long, but in speaking to those in the field, sometimes it takes that long. The U.S. provision is 90 days with provision for partial disclosure.) This is new in Canada. This is a fishing expedition. (Government answers that this is not a fishing expedition because authorities cannot see the data unless there is a warrant.) One reply is that if not a fishing expedition, it is stocking the pond procedure. Finally, what penalties are there for lack of compliance by police officer or persons subject to the order?

(iv) E-mail and other non-oral private communications

Consolidation of legal access provisions into Part VI is a good idea. Concern was expressed that the proposed new offense for making a visual recording is too widely worded. It appears it would cover legitimate video surveillance by private investigators. It would also have a chilling effect – for example, people often bring video cameras to public demonstrations.

Proposal with Respect to Compelling Interception Capability and Access to Subscriber Information.

There were concerns that putting technical ability ahead of legal authority leads to technical/legal inevitability With respect to the government-industry forum, a number of questions arose. Will this include institutions such as libraries? There are risks involved when there is informal discussion. It lacks checks and balances. Industry will facilitate going down the path rather than asking the question: should we go down this path?

(Government answers that it still would have legislative consultations and parliamentary debate.) There should be people other than industry at the discussion table. Industry will be creating technology to move toward the legislative plan. Forcing industry to create technology with holes may not be the best infrastructure. We would have to build another infrastructure to secure the holes. (Government answers that this would not weaken the infrastructure. The forum would only take place after the legislation is enacted, and the forum would discuss what is technically possible.)

What is the cost estimate? Why should the private sector pay at all? Cost might be a significant check on police. (Government answers that there is much publicly available information regarding the costs in other jurisdictions, but it does not have the information available today. Also, there are ongoing talks with ISPs so it can't produce concrete figures at this time. As to why the private sector should pay, it draws an analogy with safety features mandated for car manufacturers). One response is that the car manufacturer example is not analogous. Telcos are not in the business of selling intercepts.

A police representative provides replies to above queries. Currently, when faced with the challenge of interception, the police sit down with telcos and work out a solution acceptable to both sides. There is a long history of cooperation which will continue with dialogue. With respect to costs, we all pay tax dollars to retrofit. The cost of engineering interception is a fraction of the cost of retrofitting. With respect to the concern regarding technical ability leading to inevitability of access, we already have the authority now to obtain access; so intercept capability does not lead to inevitability of access.

The proposal converts a private communication infrastructure intended for public use, into a latent surveillance system. Government answers that it depends the purpose for which the infrastructure is being used.) There are so many different types and sizes of TSP's that the proposals may be inequitable. (Government answers that there are mechanisms to address this – for example, very small TSP's.) Criminals will just use these TSP's.

Concern was expressed regarding which groups will or will not be exempted. There should be clarification with respect to this. Will non-profit community networks be exempted? (Police answers that currently they would provide equipment in those cases.) Will religious networks be exempted? Will wireless in-home guests and trade unions be exempted? (Government answers that these are not public networks and so they will be exempted.)

What is the justification for full vs. partial exemptions? (The answer is that the list of entities on slide 17 is rarely involved and entities on slide 16 are more often involved.) A question was posed seeking empirical data supporting this position but the response was

that no answer could be provided.) Does this create a double standard? For example, if someone has the resources to create a private network, it will be exempted. (The government answered that this was not the case because the proposals do not affect the law regarding legal access.)

Where is the empirical evidence that there is a problem with the current state? (The government answers that we can't respond without jeopardizing investigations and that statistics are not kept. This is not an issue of whether interception should be done, but when there is authorized interception, how it can be carried out in a timely way and at lower cost.) We are paying for this in a hidden way. How can the public assess whether the cost of intercept capability is worth the benefits without data? This is a radical departure from how we do surveillance. It is not "normalizing" surveillance. If intercept capability is already being built into new technology, are we already getting this for free? (The police answer is that not all TSPs are cooperative although many are.) Is this not the result of a de-regulated telco industry? The government notes that the proposed requirement re removal of encryption would not apply to subscriber applied encryption such as VPN's.

Subscriber Information

The government states that they are looking for clarification of authority to receive information. CRTC already gets this information. Concern was expressed that this should not be disclosed currently without authorization. Who are the ISPs who are disclosing this information? How does this fit with PIPEDA and the obligation to keep this information private? Should this information only be available in exigent circumstances?

It is shocking that TSPs are already providing this information contrary to privacy laws. This is in effect a national database, except it is held by the TSPs instead of the police. This is like a warrantless search – if I choose to be unlisted, I'm entitled to anonymity. The provisions are not tied to an offence or investigation and are contrary to my rights.

Re last point above: An example was given of using a nickname in a chat room discussing the US war on terrorism to avoid being "flamed" or put on a watch list. Police can now obtain identity. (The police answer is that they would only obtain identity as part of a larger investigation, and not on those facts alone.)

The proposed safeguards of oversight and audit are not adequate. Complaint-based oversight is not effective. (The police answer is that inappropriate use would result in immediate dismissal.) One reply is that police have used information inappropriately before (e.g. by an officer in B.C. who used licence plate numbers of cars in the parking lot of an abortion clinic to obtain information about owners).

How will I be protected if information is sent offshore? How will this information be shared, for example, with other databases? There is not even a threshold of grounds for suspicion – this is not innocuous when it ends up on a database and could thereby create opportunities for identity theft. What protection would there be if someone wanted to send a tip by anonymous e-mail? Police could obtain the identity.

END OF REPORT OF PROCEEDINGS

ONLINE SOURCES

Lawful Access – Consultation Document. 2002. Department of Justice, Industry Canada, Solicitor General of Canada. August 25.
http://www.canada.justice.gc.ca/en/cons/la_al/consultation_index.html

Lawful Access FAQ. (Last Update: 2003). Department of Justice, Canada, August 14.
http://www.canada.justice.gc.ca/en/cons/la_al/summary/faq.html

Lexinformatica Lawful Access infopage. <http://www.lexinformatica.org/cybercrime>
Summary of Submissions to the Lawful Access Consultations. 2003. Department of Justice, Canada. April 28.
http://www.canada.justice.gc.ca/en/cons/la_al/summary/index.html

GOVERNMENT OF CANADA SOURCES (For discussion purposes – Not for further distribution)

The letters shown will be used to refer to these documents.

Distributed prior to the March 15 Meeting:

A: Lawful Access: Legal Review. 2005. Follow-up Consultations: Criminal Code Draft Proposals. Department of Justice, Canada. February- March.

B: Lawful Access – Amendments to the Competition Act. 2005. Competition Bureau, Government of Canada. March.

C: Lawful Access Proposals. 2005. Proposals with Respect to Compelling Interception Capability and Access to Subscriber Information. March.

Presented at the March 15 Meeting and Subsequently Distributed Afterwards in Hard Copy

D: Combating cyber-crime: the context. 2005. Department of Justice, Canada. March.

E: Transmission Data: Considerations for Criminal Law. 2005. Department of Justice, Canada. February.

F: Courriels: Facteurs a Consiferer en matiere de politiques de droit penal. 2005. Ministere de la Justice du Canada. Mars.

G: E-mails: Considerations for Criminal Law Policy. Department of Justice, Canada. March 2005.