Consultation on Lawful Access
Deliver By E-Mail: la-al@justice.gc.ca

November 15, 2002

Lawful Access Consultation
Criminal Law Policy Section
5th Floor
284 Wellington Street
Ottawa, Ontario, K1A 0H8

Subject: Consultation on Lawful Access

Thank you for the opportunity to comment on the proposals to provide for capability to law enforcement agencies to intercept communications and to provide for search and seizure of information pursuant to legal authority.

With approximately 8500 members, CIPS is Canada's largest association of IT professionals, representing the interests of IT professionals to industry and government. Through the volunteer efforts of its members, CIPS is involved in a number of initiatives relating to public policy, setting standards within the IT profession and providing assistance to its community. Our advocacy role is intended to reflect the public interest as well as that of our members.

Preamble

Privacy is a right upon which many other democratic rights are founded. For example, the ability to participate in private political discourse without fear of surveillance by the state is founded in part in the privacy rights of the individual. As a result, privacy is a cherished value among Canadians. This attitude of Canadians has been validated by many surveys over the past decade.

At the same time, CIPS recognizes that privacy is not an absolute right. The privacy rights of individuals must be tempered with the reasonable information requirements of the state (eg., census information).

Law enforcement activities (including related justice activities) are, for the most part, hostile to the individual's privacy interests. When a crime is committed, or thought to have been committed, activities are initiated that result in individuals coming under a great deal of scrutiny. We are not only talking about the privacy rights of those charged or convicted. Depending on the nature of the crime, the victim, friends and family members and others thought possibly to be perpetrators are also investigated.

Finally, the court system is open to the public and, with few restrictions, is reported upon by the press.

Notwithstanding the intrusive nature of the law enforcement and justice system, the Canadian law enforcement system is a reasonable, and sometimes a necessary, intrusion into the lives of Canadians with the result that a Canadian society, as we know it, is maintained.

Notwithstanding the justifiable intrusiveness of the justice system, the proposed powers for law enforcement agencies must be subject to civilian and judicial oversight.

Summary

Against this backdrop of genuine needs of law enforcement and the scepticism of the Canadian public, CIPS will present a number of concerns and propose a number of counter-balancing measures to mitigate the concerns.

CIPS will raise concerns or make suggestions with respect to:

- definitions for law enforcement and service provider.
- concern that the proposals can be easily circumvented by those under surveillance by using encryption technology
- concerns about disclosure of investigatory materials to law enforcement agencies in other countries
- concern that a Cabinet Minister does not represent citizen's interests during the Regulation-making process.
- concern about who might have access to investigatory materials after they are collected
- commentary that the investigatory material might be presumed to contain personal information and be subject to access under the *Personal Information Protection and Electronic Documents Act*
- concern about the proposal to establish a subscriber database, and
- identification of additional areas of concern with respect to illegal devices and the need to exercise caution so that innocent distribution of a virus is not criminalized, nor is possession for legitimate research purposes.

CIPS will also suggest that there should be a number of new offences with respect to the secondary use and disclosure of the investigatory materials.

The Lawful Access Consultation

As a general observation, we find the consultation document lacks justification for the proposed lawful access measures and lacks specific problem statements that need to be addressed, nor does it contain reasonable counter-balancing measures to protect the public interests and to prevent misuse of the proposed powers.

Admittedly, CIPS members for the most part, are not lawyers. But litigants seem to have the ability to seize electronic records where necessary. As a result, CIPS questions why law enforcement agencies believe the current tools to be inadequate.

Notwithstanding the general concerns of CIPS, we believe that it would be unreasonable not to provide some additional tools to law enforcement agencies to ensure that investigations are not unreasonably hindered by virtue of the fact that the medium is the online world. We also believe that some parts of the proposal cannot be dismissed without further analysis. Therefore we provide more detailed comment below.

CIPS would take a very different stand on the issue of lawful access if it were not for the requirement for the law enforcement agency to obtain a Court order to produce the records. Any attempt to weaken this safeguard would be viewed by CIPS as contrary to the "public good".

Investigatory Materials

In this response, we use the term "investigatory materials" to describe electronic communications that are intercepted, stored and disclosed to a law enforcement agency under the authority of a search warrant, Order to Produce, or other legal instrument.

Definition of Law Enforcement

The definition of "peace officer" under the Criminal Code is sufficiently broad that it includes many officers that are better characterized as compliance officers. Indeed the definition of "peace officer" includes the mayor of a community. Many provincial statutes confer "peace officer" status on compliance officers. Our view is that the proposed powers should be restricted to municipal, provincial and national police officers and bona fide investigators of national security agencies.

Furthermore law enforcement agencies that might take advantage of the proposed powers are not defined. There are many Canadian law enforcement agencies that might be better characterized as compliance agencies. Even where these compliance agencies have the power to lay charges or make arrests, the proposed powers should be restricted unless the compliance agency has turned the investigation over to a municipal, provincial or national police force, and there is conspiracy involved or electronic communications are fundamental to the commission of the crime.

Finally, not all investigations undertaken by police officers are law enforcement investigations. Police officers will sometimes conduct investigations of other police officers in their role as an employer (eg., preparation for a grievance or worker's compensation hearing). Orders to produce should not be available under these circumstances.

Definition of Service Provider

The consultation paper refers to the problem, from a law enforcement perspective, posed by the multitude of service providers and the need to have some sort of central registry to allow law enforcement agencies to efficiently identify which service providers should be served with an Order to Produce should one of their subscribers come under surveillance.

The proponents of this proposal seem to have greatly underestimated the magnitude of the problem by apparently overlooking at least two potential groups of service providers. Arguably, every employer and other organization that provides their own telecommunications (voice over IP) and Internet services will be required to provide intercept capability and to register and update the registry with subscriber information. Indeed the federal government is a very good example of this with hundreds of thousands of e-mail accounts and connections directly to the Internet. In this example, should a federal employee come under surveillance under these provisions, their employee accounts might also come under surveillance.

Another group of potential service providers are those that operate discussion groups on private web sites and virtual communities where people with like interests share ideas. The public can register for these virtual communities without authentication making it virtually impossible for those service providers to register their subscribers in a national database.

The end result appears to be a patchwork of coverage.

Rapidly Evolving Environment

While the consultation paper alludes to technological developments that affect lawful access, the consultation does not provide any assessment of the nature or scope of the problem, the effectiveness of the proposals, and whether there are options that might be considered to mitigate the problem.

To underscore this concern that the proposals do not address specific problems, many wrongdoers are smart enough to use encryption and defeat the intent of the proposed surveillance. CIPS is not suggesting that possession of encryption technology should be illegal, or that developers should provide a "back door" for law enforcement. But we are suggesting that the proposed measures can be easily circumvented.

Of even greater concern is the statement on page 4 that "the global nature of these technologies can create significant jurisdictional problems in criminal and terrorist investigations". This comment presupposes that there must be sharing of information with other countries. CIPS recognizes that mutual assistance treaties are in place between Canada and other countries. However, this document does not discuss the controls and over-sight mechanisms that are, or should be, in place to ensure that sharing of information is reasonable. Increasingly, the U.S. is demonstrating an unreasonable position on the issue of trans-border flow of Canadian residents. This is evident by the travel advisories that have been issued by the Government of Canada.

There is no reason to believe that the U.S. government will temper their demands for information about persons under investigation for serious, as well as, minor offences. As a result, we believe that there should be limited sharing of information extra-territorially. CIPS proposes that before initiating any surveillance where the investigatory materials are likely to be shared extra-territorially, the search warrant, subpoena or other legal instrument authorizing the activity must be approved by a superior court judge.

Requirement to Ensure Intercept Capability

Regulation is a method of implementing law that does not undergo the same level of scrutiny as that of a statute.

While CIPS does recognize that Regulations are an appropriate mechanism to implement technical standards, we also believe that the process as described on page 8 is biased in favour of industry concerns (as represented by Industry Canada) and law enforcement (as represented by the Solicitor General). As the Solicitor General cannot effectively represent the interests of both citizens and law enforcement at the same time, no one at the Cabinet table will advocate on behalf of citizens in the process of making Regulations. We consider this to be a serious deficiency in the proposal.

On the issue of reimbursement of the service provider, many organizations are called upon to monitor and report certain types of activities (eg., financial institutions are called upon to report certain types of financial activities, and all organizations are required to produce records when required to do so by Court order) without reimbursement. The proposal requires more of the service provider than monitoring or reporting, but the requirement to participate with law enforcement agencies is a civic duty and should not be reimbursable. In the absence of any argument that the communications service providers are faced with an unjustified financial burden, this appears to be a cost that should be borne by industry. Policy makers must also be mindful of the effect that the above discussion on the definition of service provider might have on the proposal.

Access to Investigatory Materials

The lawful access proposals referred to in the consultation are predicated on the assumption that the information needs of the state sometimes must take precedence over the competing privacy rights of individuals. But there are other facets of privacy that need to be considered.

Privacy is predicated on the notion that personal information should not be used for purposes other than those for which the information was collected. It is apparent to CIPS that various parties may seek access to the information collected by the service provider for reasons other than the original purpose.

Presumption That Record Contains Personal Information. Where an individual is under surveillance for activities that are unrelated to employment (eg., laundering of personal funds), it is our view that the records should be presumed to contain personal information of the person under investigation and must be protected.

If one accepts the position that the investigatory materials contain personal information, one must also accept that these records are highly sensitive because of the context in which they are collected. Records that are collected as part of an investigation into a possible violation of law are considered to be particularly sensitive by virtually all privacy laws.

Public policy makers must also consider that not all of those under surveillance are actually involved in wrongdoing. For example, innocent parties may be put under surveillance solely because of their relationship to the suspected individual. Or troubled teenagers may be involved in proliferation of viruses and therefore be justifiably under surveillance. But their communications may also communicate on a variety of other topics that affect troubled teens including suicide, sexual activity and disease. It would be an unjustified invasion of privacy if the investigatory materials were subsequently used for unrelated secondary purposes (such as victim impeachment during a sexual assault trial or for job applicant screening).

In other circumstances, the communications under surveillance may be subject to solicitor-client or some medical privilege. These records should be segregated and access should not be provided unless first screened by a judge.

For these reasons, secondary access and use of the information provides a significant privacy threat to those under surveillance. We propose the following information access schema.

Law Enforcement. The law enforcement agency obtaining the order to produce, or other instrument which requires the service provider to collect and disclose the personal information should have access consistent with the provisions of the Order.

Service Provider. The service provider has no right of access to the investigative materials except as provided in the Order to Produce. Normally, this access should be restricted to that access which is required to assist the law enforcement agency.

Person Under Surveillance. The person under surveillance should have access to the investigatory materials under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) after the surveillance has been completed and the person is advised of the surveillance. This right of access may be restricted by the Order to Produce. This is unlikely to interfere with a law enforcement investigation because the individual will have received a copy of the investigative materials (eg., e-mail messages) in the course of going about their day-to-day activities. However this right of access will allow the individual to review the surveilled communications from the perspective of the law enforcement investigation.

This requirement suggests that once a service provider is required to collect and store communications in accordance with an Order to Produce, the service provider or the law enforcement agency is required to securely maintain that collection for a period of time that is long enough for the individual to seek access to their personal information. Many privacy laws consider the minimum retention period for personal information to be one year after last use.

Employer. Employers may seek access to the investigative materials particularly where the employer has provided the communications equipment or service. Where the individual is investigated for activities unrelated to employment, consideration should be given with respect to employer right of access. Increasingly, some countries have restricted employer's right of access to employee e-mail in favour of employee privacy. For example, the Regulation of Investigatory Powers Act 2000 in the United Kingdom only allows monitoring of e-mail where there are reasonable grounds to believe that both the sender and recipient have consented to the monitoring.

Third Parties. Various third party (private investigators, lawyers, insurance companies, etc.) interests could be advanced by access to the investigatory materials. While it is reasonable for the state to seek access to records involving wrongdoing, it must be remembered that the surveillance will capture communications on a wide range of other topics. So that individuals are not pressured into consenting to the third party access, it should be an offence for a third party to request consent for access to investigatory records.

Other Mechanisms to Provide Subscriber and Service Provider Information

CIPS recognizes that it is not an easy task for law enforcement to determine the local service provider identification (LSPID) information. Nonetheless, CIPS believes that a subscriber database is an unwarranted intrusion into a person's private realms. Individuals have a right to be anonymous, insofar as it is possible, on the Internet. There are bona fide reasons for this ranging from privacy (eg., a person living in a small resource-based community might want to keep contributions to an environmental group private), to reduction in profiling activities. At one point, industry sought support for information on the outside of the e-mail "envelope" to be public and not subject to privacy laws. This suggests that they would welcome the opportunity to provide for matching of all persona that an individual might possess.

CIPS does not accept the recent CRTC approval of conditions under which Bell Canada could release LSPID information. The CRTC approval does not necessarily represent a broad consensus of Canadians on this issue.

CIPS previously noted (in the section on Definition of Service Provider) the significant problem of identifying who is covered by this proposal (eg., does it apply to employers and to virtual communities). You will recall that the service providers for virtual communities do not require authentication of a subscriber before providing services. Unless their business model is changed, the national registry will be a patchwork at best.

The notion of a national registry is predicated upon the notion that law enforcement must be able to accurately identify their targets in that database. That would suggest that service providers would have to collect and report more than a name and address and subscriber identifier. It is our view that the Canadian public will find the collection of a national identification number (such as the social insurance number or a new national identifier) to be unacceptable.

In the final analysis, CIPS believes that the public has a right to anonymity on the Internet (insofar as that is possible) much the same as the public can use cash for anonymous transactions in the real world. There is nothing sinister about this and it is repugnant to force citizens to register before undertaking lawful activities.

Compliance Mechanisms and Counter-Balancing Proposals

Scope of Proposed Powers. The proposed powers should be available only to police officers and intelligence officers who are investigating serious crimes such as organized crime, money laundering and terrorism where there is evidence that electronic communications are being used to conduct criminal activity. The powers should not be available for "fishing expeditions" nor should they be available for relatively minor offences.

Civilian Oversight. CIPS believes that approval of legal instruments by a justice of the peace is not a sufficient safeguard. At a minimum, the "legal instrument" providing access should be an order of a Superior Court. We also propose that orders to produce and other legal instruments should be subject to civilian oversight. We have not provided details how this might work but it should likely be a retroactive oversight mechanism by a special committee that reports to Parliament.

As already mentioned, there should be a senior Minister to represent the interests of citizens in the regulation making process and civilian over-sight.

Audit Trails. Audit trails should be required for all access to the investigatory materials by law enforcement, services provider and third parties.

Safeguards to be Provided by Service Provider. To prevent unauthorized access to the investigatory materials while stored at the service provider's site, the investigatory materials should be encrypted with access only provided to authorized individuals. An audit trail of all activities should be produced.

Offences. To protect the public from potential abuse and misuse of the investigatory materials, CIPS proposes that a number of new offences should be created. These offences should apply equally to law enforcement agencies and to businesses (eg., private investigators and insurance companies to name two), organizations and the public.

CIPS proposes that the following should be offences:

- Seeking access (eg., simply asking for access) to electronic communications without an Order to Produce or similar legal instrument.
- Collecting electronic communications without a legal instrument allowing the organization to do so.
- Disclosing electronic communications collected under the authority of a legal instrument, to any person not explicitly provided access in the legal instrument.

- Accessing, or attempting to access, investigatory materials under false pretences.

Penalties should be similar to those under the Personal Information Protection and Electronic Documents Act. In serious breaches of confidentiality and the above-noted offences (eg., those involving health or law enforcement information, or undertaken with a view to discredit an individual for small "p" political purposes), the penalties should include the potential for incarceration.

Employee Rights. Where an employer (as a "service provider") might be served with an Order to Produce records of an employee, the employers should be prohibited from disciplining the employee solely on that basis.

Illegal Devices

The consultation suggests that there should be new offences in relation to illegal devices such as viruses. CIPS believes that viruses and similar devices do need controls and offences do not seem unreasonable. But we do suggest that care must be taken not to prohibit the legitimate activities of bona fide researchers and companies that possess these devices for analytical purposes and to develop safeguards (eg., create signature files so that the viruses can be detected and destroyed).

Nor should a person be guilty of an offence if they have an undetected virus or other device residing on their computer that is transmitted without their knowledge.

An area of illegal devices that may need additional attention is "spyware". These products collect information about a computer user's browsing habits (known in the industry as "click-stream" data) and surreptitiously transmit it to an information broker. Some browsers and media products reportedly have this capability. The software end user license agreement (EULA) refers to this practice, however, the surveillance is surreptitious and, in our view, unethical. The practice poses certain legal issues with respect to one person consenting to surveillance (if he or she is aware of it at all) on behalf of all users of that computer, or where the person accepting the terms of the EULA is a minor. For these reasons, we believe that these products should be banned from manufacture, sale or distribution (eg., preloaded on computers) in Canada.

Unethical and fraudulent businesses are engaged in mass mailing (millions) of unsolicited e-mail for commercial and other purposes (SPAM). This activity results in lost productivity and increased salary costs while employees process these messages. It also increases costs to the organization to deploy increased storage capacity. Our view is that this activity should be a Criminal Code offence. Care should be taken to ensure that legitimate businesses that send unsolicited e-mail to others that reasonably have, or ought to have, an interest in the product or service are not in contravention of the law.

Related to the issue of SPAM is the activity of those who misrepresent themselves. One way this is done is to use someone else's e-mail address in the "reply to" line of an e-mail. Our view is that this constitutes theft of identity and it damages the reputation of the person whose identity has been usurped. In extreme cases, it may result in the innocent party's e-mail and Internet services being terminated. Our view is that misrepresenting one's self as the sender of an e-mail for unauthorized purposes should be a criminal offences that is similar to fraud. Care should be taken not to criminalize providing bogus information where the intent is to protect one's privacy.

Interception of e-Mail

The consultation paper suggests some ambiguity in law with respect to a reasonable expectation of privacy. CIPS believes that e-mail should be afforded the same privacy protection as regular mail and telephone conversations. It is our view that it should be an offence to intercept or otherwise access e-mail at any point during the transmission between the sender and recipient unless the access is authorized by a search warrant or subpoena or other legal instrument.

Summary

In closing, CIPS members have a tremendous respect for the job done by the law enforcement community. But at the same time, we believe that the proposals in their current form will not work. More importantly however, we believe that the proposals do not contain reasonable safeguards to counter-balance the powers of the state and, as a result, are unwarranted in their current form.

We hope that this letter provides constructive input in the dialogue.

Sincerely,

CANADIAN INFORMATION PROCESSING SOCIETY

Charles W. Wordsworth, I.S.P.

President