

Public Interest Advocacy Centre

Comments on the Federal Government's “Lawful Access” Consultation Document

December 16, 2002

CONTACT:

Philippa Lawson
Senior Counsel, PIAC
1204 – 1 Nicholas St.
Ottawa, ON K1N 7B7
(613) 562-4002 x.24
plawson@piac.ca
<http://www.piac.ca>

Table of Contents

INTRODUCTION..... 3

GUIDING PRINCIPLES 3

GENERAL CONCLUSIONS 4

 LACK OF SUPPORTING DATA 5

 TECHNICAL OR LEGAL PROBLEMS? 5

 TECHNOLOGICAL NEUTRALITY 5

MAINTAINING LAWFUL ACCESS CAPABILITY VS. INCREASING LAWFUL ACCESS CAPABILITY 6

 THE COUNCIL OF EUROPE CONVENTION ON CYBER-CRIME 6

 LACK OF CORRESPONDING PRIVACY SAFEGUARDS 7

INTERCEPT CAPABILITY 8

EMAIL INTERCEPTION 10

 REASONABLE EXPECTATION OF PRIVACY 10

 INTERCEPTION OR SEARCH AND SEIZURE? 10

ACCESS TO SUBSCRIBER AND SERVICE PROVIDER ID 10

 DEFINITIONS 10

 OTHER MECHANISMS TO PROVIDE SUBSCRIBER AND SERVICE PROVIDER INFORMATION 13

PRODUCTION ORDERS..... 13

 GENERAL PRODUCTION ORDERS 14

 PRODUCTION ORDERS FOR “TRAFFIC DATA” 14

PRESERVATION ORDERS 15

VIRUS DISSEMINATION 16

EXTRA-TERRITORIALITY..... 17

CONCLUSION 17

Introduction

The Public Interest Advocacy Centre (PIAC) is a national non-profit organization devoted to the representation of consumer interests in matters involving public utilities, essential services, and public interest issues of broad application to Canadians. PIAC has developed a strong record of consumer advocacy since its inception in 1976, and is widely recognized as an important and influential voice for ordinary consumers in a variety of marketplace issues. Over the past decade, PIAC has become a leading advocate of consumer privacy interests, in the context, especially, of the electronic marketplace. PIAC is governed by a distinguished volunteer Board of Directors from across the country, and is supported by member groups and donors representing hundreds of thousands of Canadians.¹

PIAC is grateful for the opportunity to comment on the important issues raised in the Consultation Document issued August 25, 2002 by the Government of Canada on “Lawful Access”. We commend the Government on its efforts to reach out to, and obtain input from, civil society through advance consultations on these issues. However, our ability to provide feedback is limited due to a lack of detail and clarity regarding the legislative proposals as well as the problems they are designed to overcome. Our comments below are therefore more general than might otherwise have been the case.

We look forward to an opportunity to review and comment on more specific legislative proposals accompanied by more substantial evidence as to their need.

Guiding Principles

The guiding principles for lawful access in Canada have already been established in the *Canadian Charter of Rights and Freedoms*, and Supreme Court jurisprudence interpreting these fundamental rights and freedoms. Under section 8 of the *Charter*, “everyone has the right to the secure against unreasonable search and seizure”, “subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society”. A significant body of jurisprudence has developed under this principle, providing helpful guidance as to where the line is to be drawn between reasonable and unreasonable intrusions by the state into the personal lives of individuals.

The Supreme Court of Canada has repeatedly confirmed the importance of privacy as an essential aspect of an individual’s liberty in a free and democratic society.² As noted by the Court,

¹ For more information, see <http://www.piac.ca>

² E.g., *R. v. O’Connor* [1995]; *R. v. Duarte* [1990]; *R. v. Dyment* [1998].

“The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communication will remain private.”³

The Court has also emphasized the importance of prior judicial authorization as an essential safeguard against undue invasion of individual privacy by the state:

“The state’s interest in detecting and preventing crime begins to prevail over the individual’s interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement.”⁴

In *R. v. Oakes*,⁵ the Court established a clear test for the determination of whether a given infringement of *Charter* rights is reasonable and demonstrably justified. This test requires a sufficiently important objective served by the infringement, a rational connection between the means and the ends, and minimal impairment of the right in question.

We agree with the Privacy Commissioner of Canada that any new privacy-invasive measure that purports to enhance security must meet the following test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.⁶

General Conclusions

Having reviewed the Consultation Document, and participated in a day-long consultation with government officials, it is PIAC’s view that the Government’s proposals for greater lawful access to private communications have not been demonstrably justified, according to the test articulated by both the Supreme Court of Canada and the Privacy Commissioner of Canada. In particular,

- it is not clear that greater access by law enforcement to electronic communications will in fact, or is even likely to, increase the security of Canadians;

³ *R. v. Duarte* [1990] 1 S.C.R. 30, at para 24.

⁴ *Hunter v. Southam*, [1984] 2 S.C.R. 145 at 166-7.

⁵ [1986] 1 S.C.R. 103.

⁶ Comments, November 25, 2002.

- the privacy intrusions that would result from these proposals are clearly significant, while the security benefit to be derived therefrom is unclear;
- it has not been demonstrated that no other, less privacy-intrusive, measure (e.g., focused on technological and/or administrative impediments) would suffice to achieve the same purpose of enhanced security.

We fully appreciate the need for law enforcement agencies to be able to protect citizens against criminal activity without undue effort. We are as interested as everyone in the security and safety of Canadians. However, we strongly oppose measures that provide law enforcement agencies with greater powers of intrusion into the private lives of individuals, without adequate safeguards against the abuse of such powers.

Lack of Supporting Data

The legislative reforms being considered are premised on a need for enhanced state power in the face of technological change and specific barriers that exist today. Yet, the government has provided little evidence to justify the significant privacy intrusions posed by increased lawful access. Without specific information as to the extent and nature of the problem(s) to be rectified, it is impossible to conduct the “cost/benefit” analysis required by the Supreme Court.

Indeed, PIAC is unable to answer most of the specific questions posed in the Consultation Document because of the lack of information provided to justify the proposals.

If evidence is available to justify the proposed measures, it should be made public, so that Canadians can weigh it and thus make informed judgements as to whether the security benefits of the measures outweighs the privacy costs. If such evidence does not exist, then there is no case for the measures in question, and they should be dropped.

Technical or Legal Problems?

The Consultation Document identifies a number of technological developments that have created problems for law enforcement investigations (p.4). It would appear that the problems in question are technical, rather than legal. If law enforcement agencies have difficulty dealing with new technologies of communication, the solution is not to lower the legal standard for interception or search and seizure; rather, it is to provide law enforcement agencies with the technical expertise they need to deal with the evolving environment.

Technological Neutrality

The proposals would effectively establish a lower standard for interception and/or search and seizure in the online context, versus in the offline context. Yet, no justification in principle has been provided applying a different standard depending on the mode of communication used.

PIAC submits that legal standards should not differ according to technology. Not only would this be unprincipled; it would lead to a situation in which the government is constantly playing legislative “catch up” with new technologies. Criminal Code standards should be designed to apply regardless of technology, and legislative reform should focus on ensuring that the standards in question are worded so as to incorporate all relevant technologies (rather than on establishing lower standards for certain types of technology).

Maintaining Lawful Access Capability vs. Increasing Lawful Access Capability

The Consultation Document states that the objective of the Lawful Access proposals is “to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies”.⁷ Yet, the proposals go much further than *maintaining* existing lawful access capabilities – instead, they would significantly *increase* the ability of law enforcement and national security agencies to intercept, search and seize electronic communications of individuals, and personal information about individuals in electronic form.

PIAC has no objection to updating Canadian legislation so that the well-established Canadian standards of lawful access to private communications and personal data are clearly applicable in the context of new communications technologies. We do, however, object to a substantial weakening of such well-established safeguards.

The Council of Europe Convention on Cyber-Crime

It is unclear to what extent the proposals in question have been driven by forces outside Canada. According to the Consultation Document, the Council of Europe *Convention on Cyber-Crime* requires that ratifying countries provide in their domestic law for Production Orders, Preservation Orders, and an offence in relation to computer viruses that are not yet deployed.⁸ PIAC’s comments on these specific proposals are set out below.

In general, however, we are concerned that some aspects of this *Convention* may be inconsistent with Canadian values, insofar as it requires provision for an unreasonable level of state incursion into the private lives of individuals, without adequate privacy safeguards. In our view, Canada should not ratify the *Convention* if to do so would be inconsistent with Canadian values and rights as set out in our *Charter of Rights and Freedoms* and interpreted by the Supreme Court of Canada.

What position did Canada take in the negotiations?

There is absolutely no information available as to the position that Canada took in the negotiations. If this information were available, it would aid in understanding and framing the lawful access proposals.

⁷ p.6.

⁸ p.5.

What are the options being considered (and not considered)?

Similarly, no information is available to understand which options were considered and rejected in the process leading to the convention signing. Why was there no pre-signing consultation to review and direct the position that Canada would take?

Lack of Corresponding Privacy Safeguards

While clearly aware of privacy concerns, the government does not appear to have made a serious attempt to weigh them against the pressure from law enforcement agencies for easier access to personal information in the electronic environment.

Privacy, as much as national security, is under attack

The same technologies that law enforcement agencies complain are hindering their ability to investigate criminal activities, have also provided the basis for an unprecedented erosion of individual privacy. Individual privacy is increasingly under assault by virtue of the vastly easier access to vastly greater quantities of personal information available electronically. We find it particularly ironic in this context that the government seeks to further erode individual privacy, in the name of the public interest. If anything, privacy protections for electronic communication should be stronger than for non-electronic communications, given the unprecedented opportunities that electronic technologies offer for surveillance and intrusion.

The Need for Privacy Safeguards

In contrast to the Lawful Access legislative proposals, is the government's recent legislative initiative on Money Laundering (*The Proceeds of Crime Act*). Just over two years ago, the federal government consulted with the Privacy Commissioner and the public on legislation designed to detect and deter money laundering and to facilitate the investigation and prosecution of money laundering offences. In response to concerns raised by the Privacy Commissioner and stakeholders, the government included a number of measures designed to limit otherwise enormous systemic individual privacy invasions that would have been authorized. For example, Bill C-22 (as it then was) included provisions:

- exempting lawyers from the requirement to disclose communications, where such communications are subject to solicitor-client privilege;
- requiring the police to obtain a judicial warrant in order to obtain detailed information from the new Financial Transactions and Reports Analysis Centre of Canada (FTRAC);
- limiting the use of information by FTRAC or other officials to purposes of exercising powers or performing duties and functions under the Act;
- making a punishable offence the improper disclosure of information; and
- giving the Privacy Commission oversight powers in relation to FTRAC's handling of personal information.

In contrast, the Lawful Access proposals contain no safeguards against abuse of the increased powers they would provide.

Recommended Safeguards

The proposal assumes almost unlimited levels of citizen trust in law enforcement and national security agencies; trust that historically has not always been deserved. It argues for the need to infringe upon individual rights, suggesting this will enhance collective public security. As noted above, PIAC does not consider that the proposals have been adequately justified.

Should they nevertheless proceed, any proposals for greater access by law enforcement agencies to private communications and information must be accompanied by strong oversight mechanisms that ensure public accountability, transparency and scrutiny. This oversight should require routine reporting on measures undertaken in the name of law enforcement and national security and an accounting of the efficacy of these measures. Such reporting would enhance public confidence in the government and its agents exercising their rights to intercept and collect personal data.

Specific and severe penalties for improper use or disclosure of personal data collected via lawful access, as well as for improper attempts to access personal data, should be introduced

Specific procedures should be enacted for the destruction of information seized or acquired as part of a lawful access endeavour, at a minimum these should include:

- Specific guidelines to be followed for destruction
- Specific guidelines to be followed to notify parties whose information has been intercepted

Specific procedures should be enacted for the handling of intercepted or seized information that is subject to legal privilege.

In summary, we believe that all interception and/or search and seizure of electronic communications should require judicial approval, should identify a specific target, should identify specific information to be seized/intercepted and should have a specific rationale and justification for the seizure or interception. We also believe that any orders issued should be time-limited.

Intercept Capability

The government is proposing to introduce a general requirement in legislation to ensure intercept capability, with the specific details to be contained in regulations proclaimed at the time the legislation will come into force. It is proposed that all service providers (wireless, wireline and Internet) be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies.

We recognize that there may be a need for assurance, on the part of law enforcement agencies, of the ability to intercept and monitor electronic communications upon the issuing of judicial authorization. However, the government has failed to present evidence that the deployment of this massive surveillance infrastructure is necessary. For example, we do not know how many investigations have been thwarted as a result of the lack of technical capability. Moreover, the lack of clarity regarding evidentiary thresholds, oversight and safeguards makes us unable to provide an opinion on this proposal.

The Consultation Document suggests that many of the important details of such interception capability requirement (e.g., cost recovery) would be left to regulation. It is important that any regulations be subject to full public review. We echo the call from CWTA and CAIP and request that the draft legislation and accompanying regulations be made available for a full and complete public review, and that sufficient time be provided for interested parties to assess their impact and submit comments.

Effect on future innovation and adoption of technology

It is possible that impact the proposed requirement for intercept capability will have an adverse effect on future innovation in this industry. In particular, if intercept requirements are not applied to current infrastructure but only “when a significant upgrade is made to their systems or networks”,⁹ ISPs may be disinclined to upgrade their operations or capabilities. This could limit innovation and is therefore arguably in conflict with Canadian telecommunications policy.¹⁰

Cost implications

We are concerned that the cost of constructing the surveillance infrastructure may unnecessarily burden the industry, and hence the telecommunications user. This, again, is arguably in conflict with Canadian telecommunications policy.¹¹ In any case, it is impossible for us to address this issue fully without more information as to the costs in question.

It is certain than there will be disagreement between the industry groups and others with respect to costs. Some have envisioned the ISPs assuming the costs of ‘lawful access’, others have envisioned the government providing funding through some form of authorized tariff. Either way, it is clear that the citizen, as a telecommunications user or as a taxpayer, will be responsible for the costs of ‘lawful access’. Any such costs should be minimized.

⁹ *Consultation Document* – Pg. 10.

¹⁰ Section 7 (g) - *Telecommunications Act* - STATUTES OF CANADA, Chapter 38.

¹¹ *Ibid.*, Section 7 (a-h).

Email Interception

The government seeks input on whether, or when, email constitutes a communication subject to interception, or instead a document subject to search and seizure. Different standards for access apply, depending on which approach is taken.

Reasonable expectation of privacy

Canadians have come to expect a high degree of privacy in email, despite widespread awareness of the ease with which such communications can be accessed by third parties. Increasingly, we are using email to communicate highly sensitive information, and indeed are relying on it to the same extent that we rely on postal mail. Canadians have, we submit, a similar reasonable expectation of privacy in email as they do in other forms of communication.

However, it is important to recognize the limits of the “reasonable expectation” test, where rapidly developing technology is concerned. Internet and email communications is an area in which technology and business practices have far outpaced the law. As a result, “reasonable expectations” may be based not on what is *desirable*, but rather on what we *know* to be the case, as undesirable as it may be. The legal treatment of email should not be determined by technological capability, but rather by our values as a society. If we wish to be able to communicate privately by email, without the possibility of unjustified surveillance, we should construct our laws so as to protect that desire. Principle, not technology, should guide our determination of this issue, as it did in the context of cellular telephone privacy.

Proceeding on this basis, PIAC submits that the Criminal Code should be amended to clarify that email, at least while in transit, constitutes a “private communication” under s.183. It would then be subject to the same procedural safeguards as all other interceptions under this provision.

Interception or Search and Seizure?

While in transit, interception of email is clearly just that: interception. It is a good question, though, at what point in the process of communication/delivery email is no longer a communication subject to interception, and is instead a document subject to search and seizure. The Criminal Code should be clear about when and where the line is to be drawn, if at all, between these two possibilities.

Access to Subscriber and Service Provider ID

Definitions

CNA = Customer Name and Address (in effect the identity of the subscriber).

LSPID = Local Service Provider Identification (identifies the company that provides services to the subscriber).

The government's consultation document states that, "Basic customer information such as name, billing address, phone number and name of service provider, has historically been made available by service providers without a prior judicial authorization (such as a search warrant)." ¹² Recent changes in the telecommunications sector, however, have left law enforcement agencies with a patchwork of differing and inconsistent policies among service providers, regarding the provision of this information upon request. The *PIPED Act*, for its part, permits (but notably does not require) private organizations to disclose this information upon request by law enforcement officials without judicial authorization. Instead, it is left to the government to determine what limits, if any, should apply in respect of access by law enforcement agencies to this information.

Notwithstanding the discretion afforded service providers by virtue of PIPEDA, we believe that from a public policy perspective, it is beneficial to build a clear, consistent, privacy-protective policy framework that balances all of the competing interests.

LSPID

The CRTC recently ruled on the LSPID issue in the context of telephone service providers, requiring that, in order to obtain this information from Bell Canada, a law enforcement agency (LEA) must identify its lawful authority to obtain the information, and indicate that:

- (i) it has reasonable grounds to suspect that the information relates to national security, the defence of Canada, or the conduct of international affairs;
- (ii) the disclosure is requested for the purpose of administering or enforcing any law of Canada, a province, or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing or administering any such law; or
- (iii) it needs the information because of an emergency that threatens the life, health or security of an individual, or the LEA otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property. ¹³

PIAC submits that the CRTC test for LSPID disclosure by Bell Canada is appropriate, and should be adopted in respect of other communications service providers.

CNA

On the other hand, we believe that access to CNA data should require judicial authorization. Customer name and address information can be sensitive information, depending on the context. It is not clear why we should grant law enforcement agencies unimpeded access to this information. Clearly, much of this information is already easily accessible in the marketplace, through published directories. However, many subscribers choose to protect their privacy by not publishing their contact information; in these cases, at least, individuals have a high expectation

¹² *Consultation Document* – Pg. 12.

¹³ Telecom Decision CRTC 2002-21, 12 April 2002, para.22.

of privacy regarding their contact information, and such expectations should be reflected in the standard applied for lawful access.

With respect to Internet address information, we strongly object to a lower standard of access given that the ability to link such information to identified individuals would permit the collection of a vast amount of personal information.

Some may argue that by requiring judicial authorization for CNA release, we will create a system that is expensive, inconvenient and unfairly burdens the law enforcement or national security agency. We submit that these are not the only factors to consider when drafting public policy. Rather, it is imperative in a free and democratic society to balance the legitimate needs of the state with appropriate roadblocks to protect the rights of the citizenry from incursion by the state; this may, in fact, be expensive and inconvenient and may burden the state. Freedom has a cost; we believe the state can more properly bear the burden of this cost.

Obligation to collect where none exists

We have been asked to comment on whether the obligation should be imposed on service providers to collect this information in circumstances where they are not currently collecting this information for their own purposes. This obligation would likely affect those service providers and retailers selling prepaid and other anonymous telephone cards and phones.

We would imagine, for this to be implemented, a customer would need to present approved identification to a retail clerk (e.g. a convenience store clerk) who would verify and copy down the identification; this would then be forwarded to the service provider. This would be a gross invasion of privacy¹⁴ and present even greater opportunities for data leakage or loss (and subsequent threats such as identity theft).

In discussing this point, we are struck by the fact that this proposal appears to conflict with the implicit premise of the consultation as attempting to overcome differences in legal process necessitated by technology. For example, if we require name and address to be supplied by persons purchasing pre-paid cards and anonymous wireless phones; why are we not similarly requiring persons utilizing the services of Canada Post to identify themselves? Should we not seal all Canada Post street mailboxes and require people depositing mail to present themselves at a government approved post office and present their government approved identification to a government approved counter clerk? Most correspondents would recognize the lunacy and Orwellian effect of such an unprecedented level of state intrusion.

We should not afford any lesser protection, or impose any higher burden on service providers, retailers and end users merely because they wish to avail themselves of technology solutions as an alternative to Canada Post.

¹⁴ *Comments of the Privacy Commissioner of Canada on Lawful Access*, November 25th, 2002.

Other mechanisms to provide subscriber and service provider information

The government raises the topic of ‘other mechanisms’ for law enforcement and national security agencies to access subscriber (CNA) and service provider (LSPID) information, arguing that, “the only way in which this information can be obtained is through the time-consuming and costly process of directly contacting each local carrier.”¹⁵ The Canadian Association of Chiefs of Police has suggested the concept of a national database be constructed containing CNA and LSPID information for ‘lawful access’ use.

We recognize that it is not always an easy task for law enforcement and national security agencies to obtain CNA and LSPID information. We recognize that considerable cost and effort may be expended to locate this information. However, we believe that these are not the only factors to consider when drafting public policy. Creation of a national database of any personal information, even limited to CNA information, raises the potential for misuse and should therefore be avoided.

Production Orders

In keeping with requirements under the Council of Europe *Convention on Cyber-Crime*, the Government proposes to create a new type of authorization for lawful access to documents held by a private body. A “production order” would require the custodian of documents to deliver or make available the documents within a specified period.¹⁶

The concept of production orders raises concerns about forcing private service providers into a role of agents of the state. It is at least questionable whether such “conscriptio” of third parties to carry out law enforcement activities is appropriate. It would undoubtedly interfere with the primary role of serving customers, and would effectively expand the reach of law enforcement well beyond current limits.

Three types of production order are being considered¹⁷:

- General production order
- Specific production order for traffic data
- Specific production order for CNA and LSPID data

¹⁵ *Consultation Document* – Pg. 18.

¹⁶ *Ibid.* – Pg. 10.

¹⁷ *Ibid.* – Pg. 10.

General Production Orders

PIAC does not support the creation of production orders in the absence of clear evidence showing how existing warrant powers (supplemented with assistance orders where necessary) are insufficient. Such evidence has yet to be provided.

The need for anticipatory orders, permitting law enforcement agencies to monitor transactions for a specified period of time, is also insufficiently documented. In any case, we cannot perceive a situation in which any such order would or should require a different standard than currently applies to search and seizure, or to interception of communications.

If general production orders are nevertheless created, they should be subject to the same procedural safeguards as currently apply to search warrants (or interception, where appropriate). To apply any lower standard would be to go beyond the objective of *maintaining* existing lawful access capabilities, in the new electronic environment.

Production Orders for “Traffic Data”

It is suggested that issuance of specific production orders would be subject to a lower standard than that for issuance of general production orders. In particular, the Consultation paper suggests that “the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders in light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication”.¹⁸

PIAC disagrees. First, it is not at all clear how “traffic data” in the Internet context could be stripped of content that is not available in the telephone context. Second, it is not clear that individuals have a low expectation of privacy in respect of their Internet address, at least once they know what other information about them could, or would necessarily, be transmitted along with Internet address information.

The Lawful Access Consultation document does not define traffic data. However, a definition is found in The Council of Europe Convention on Cyber-Crime. Under the Convention, traffic data is defined as, “any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.”¹⁹

It is notable that the explanatory memorandum to the Convention cautions against the simplistic notion that Internet “traffic data” can be easily separated from more substantive information in which a higher expectation of privacy exists:

¹⁸ p.12.

¹⁹ *The Council of Europe Convention on Cyber-Crime*, Article 1(d)

“... the privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person’s interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures...”²⁰

It has become apparent during the course of this consultation that it simply is not possible to clearly separate ‘traffic’ data from ‘content’ data (i.e., data that reveals much more about an individual) in the internet context. See A Pascual’s “Access to traffic data: when reality is far more complicated than a legal definition.”²¹ What looks like mere “traffic data” to a computer layperson, for example, could be a wealth of personal information in the hands of a computer expert.

Given that internet ‘traffic data’ can be so rich in information about an person’s lifestyle, interests, views, etc., the standard for lawful access to such data should be at least as high as currently required for interception of communications or searching of records. Otherwise, the government will not be *maintaining* current standards of lawful access, but will in fact be *expanding* them.

As noted by the Privacy Commissioner of Canada, George Radwanski, “Agents of the state in Canada cannot order Canada Post to photocopy the address on every envelope we send, nor can they order bookstores to keep a record of every book we buy, let alone of every page of every magazine we leaf through. There is no reason why they should be able to exercise such powers with regard to every e-mail someone sends or every Web site he visits.”²²

Preservation Orders

Preservation orders do not currently exist in Canadian law. They are being proposed pursuant the Council of Europe *Convention*, so as to provide law enforcement with a further tool of access. A preservation order would require the service providers to store and save existing data specific to a transaction or client. The order would be temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a judicial warrant to seize the data or a production order to deliver the data.²³

²⁰ *Explanatory Memorandum to the Convention on Cyber-Crime*, para. 221.

²¹ <http://www.it.kth.se/~aep/private/cnglobal2002-escuderoa.ppt>

²² *Comments of the Privacy Commissioner of Canada on Lawful Access*, November 25th, 2002.

²³ *Consultation Document* – Pg. 14.

No data has been provided to justify the creation of this new order, which constitutes a limited form of data retention. Without clear justification, it should not be adopted.

While the proposed Preservation Order does not raise the same concerns as would routine, longer-term retention of data as proposed in other jurisdictions, it is a step in that direction and could become a “back door” method of obtaining judicial authorization for access, circumventing the higher thresholds that would apply for standard warrants.

We do not believe that a clear case has been made to support the introduction of data-preservation orders. No statistics have been introduced, no rationale has been offered beyond simple reference to the Council of Europe Convention on Cyber-Crime. In any case, the creation of this new type of order would clearly constitute an expansion, rather than a maintenance, of existing lawful access capabilities, and should be rejected on that basis alone.

Virus Dissemination

The Council of Europe Convention on Cyber-Crime requires signatory states to criminalize the creation, sale and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offences specified in the Convention, whether or not the virus has been deployed or has caused any form of mischief.

Further, in order to ratify the Convention, new offences in relation to illegal devices (such as viruses) would have to be added. These could include importation, procurement for use, and otherwise making available an illegal device as defined in the Convention.

We generally support the prohibition against viruses, as contemplated by the government. However, we have some concerns about the application of the proposal with respect to a virus that has not been deployed and has not caused any mischief. Some software or devices, due to programming errors (commonly referred to as ‘bugs’) or poor programming technique may fall within scope of this prohibition. Care should be taken to appropriately circumscribe the definition of virus and non-deployed or contingent virus.

In addition, care must be taken not to prohibit the legitimate activities of individuals and companies that possess these devices for analytical, research, design, educational, or anti-virus purposes. Nor should a person be guilty of an offence if they have an undetected virus or other device residing on their computer without their knowledge. Any provision outlawing possession of viruses should be carefully drafted so as to ensure that innocent individuals will not be caught.

Extra-Territoriality

The consultation paper details that the Council of Europe Convention on Cyber-Crime calls for the criminalization of certain offences relating to computers, the adoption of procedural powers in order to investigate and prosecute cyber-crime, **and the promotion of international cooperation through mutual legal assistance and extradition in a criminal realm that knows no borders.**²⁴

We have serious concerns regarding the risk of Canadians being subject to non-Canadian laws based upon a request from another jurisdiction. Canadian law enforcement officials should only enforce Canadian laws and not assist in the enforcement of foreign laws that are substantially different.

Conclusion

The Canadian government, through the *Canadian Electronic Commerce Strategy* and the policy objectives of the *Telecommunications Act* has actively encouraged the adoption of new technologies within the Canadian marketplace. Indeed, we rank ahead of many other countries in terms of penetration and user acceptance and even cost in the internet and telecommunication sectors. These accomplishments have brought Canada well deserved praise as well as obvious economic benefit. It would seem that these same new technologies are now being used to justify a potentially invasive state surveillance regime under the guise of ‘lawful access’.

We agree that new technologies necessitate updated legislation, so as to ensure that they are not inappropriately excluded from existing provisions. However, we do not see any reason why electronic mail should be subject to a lower standard of protection than telephone calls or regular mail. We do not see why Internet browsing should be subject to a lower standard of protection than book purchasing or researching in a library. We do not see why our movements should be subject to tracking merely because we choose to use a cellular phone or other wireless device.

Canadians should not be subject to greater monitoring or scrutiny just because they choose to avail themselves of new technologies and convenience. Criminal law principles, including standards for lawful access, should be technology-neutral.

Throughout this consultation process the government has not demonstrated why the proposed measures are necessary, how they are reasonable or that there are no less-intrusive alternatives. Such evidence is required in order to meet the test set out in the *Charter of Rights and Freedoms*, as well as to convince civil society of the appropriateness of the proposed measures. After a

²⁴ *Consultation Document* – Pg. 5.

review of the consultation paper and participation in the roundtable activities, we find ourselves left with more questions than answers. We cannot support the proposed new measures for lawful access in their current form given the lack of supporting data, the lack of adequate privacy safeguards inherent in them, and the significant expansion in lawful access that they would permit for one type of technology. We do not believe that the proposals, as currently constituted, meet the test set out by the Supreme Court of Canada for reasonable and demonstrably justified limits on the right to be free from state surveillance.

We therefore call upon the government to take the following steps, if it wishes to pursue this matter further:

- Publish all background materials relating to the Council of Europe Convention on Cyber-Crime, including documents detailing Canada's position, and explanatory memoranda relating to the Canadian implementation of the convention;
- Provide empirical evidence and full justification for all components of the lawful access proposals;
- Publish draft legislation and accompanying regulations for further consideration and feedback by stakeholders, so that we know what precisely is being proposed;
- Allow sufficient time for a full, thorough and informed public consultation.

All of which is respectfully submitted,

original signed

Philippa Lawson
Senior Counsel
Public Interest Advocacy Centre