

Privacy Commissioner of Canada

The Privacy Commissioner of Canada, George Radwanski, sent the following letter to the Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada, the Honourable Wayne Easter, Solicitor General of Canada, and the Honourable Allan Rock, Minister of Industry, regarding the "Lawful Access" proposals.

November 25, 2002

I welcome the opportunity to comment on the "Lawful Access" proposals that have been put forward by the Minister of Justice and Attorney General of Canada, the Solicitor General of Canada and the Minister of Industry.

The proposals that have been presented in the consultation paper are of fundamental importance to Canadians. Under the so-called "lawful access" proposal that the federal government has put forward, our use of the Internet and our electronic communications would be subject to unprecedented scrutiny

The interception and monitoring of private communications is a highly intrusive activity that strikes at the heart of the right to privacy. If Canadians can no longer feel secure that their web surfing and their electronic communications are in fact private, this will mark a grave, needless and unjustifiable deterioration of privacy rights in our country.

I do not suggest that privacy is an absolute right. I recognize that there may sometimes be a need for some new privacy-invasive measures to enhance security and allow law enforcement agencies to investigate crimes and threats to public safety. But proposals for any such measures must be evaluated calmly, carefully and on a case by case basis.

The burden of proof must always be on those who claim that some new intrusion or limitation on privacy is necessary.

I have suggested that any such proposed measure must meet a four-part 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.

The consultation paper cites two main reasons for the measures it proposes:

- a need on the part of law enforcement and national security agencies to "maintain lawful access capabilities" in the face of technological developments; and
- a need to enable Canada to honour its international commitments, particularly the Council of Europe *Convention on Cyber-Crime*.

It is apparent to me, however, that what is being requested here are significantly new and

[About Us](#)

[What's New](#)

[Commissioner's Findings](#)

[Media Centre](#)

[News Releases](#)

[Key Issues](#)

[Miscellaneous](#)

[Resource Centre](#)

[Individuals](#)

[Business](#)

[Publications](#)

[Annual Reports](#)

[Provincial/Territorial](#)

[Links](#)

[Health Links](#)

[Privacy Links](#)

[Speeches](#)

[Privacy Legislation](#)

[Fact Sheets](#)

[FAQs](#)

[Privacy Quiz](#)

[To Reach Us](#)

enhanced powers of access to the private communications of Canadians that go far beyond maintaining the capabilities and authorities that law enforcement and national security agencies may have had in the past.

What's missing is evidence demonstrating that there is, in fact, a serious problem that needs to be addressed. Lacking any evidence of serious problems requiring correction by invading the privacy of Canadians, it is not possible to be persuaded that the proposals address these problems effectively, proportionally, and in the least privacy-invasive manner possible.

As a first step, I would strongly encourage the three departments involved in this proposal to present a clear statement of the problems faced, along with empirical evidence supporting the need for enhanced interception and surveillance powers as proposed in the consultation paper. The arguments advanced in the consultation paper are completely insufficient.

I am equally unconvinced by the argument that international commitments require Canadians to submit to an enhanced domestic surveillance regime. This is especially the case because one of the main purposes of the Council of Europe *Convention on Cyber-Crime* is to facilitate information-sharing among law enforcement agencies in the signatory countries. This raises the spectre of intrusive surveillance activities carried out upon Canadians by Canadian law enforcement and security agencies, yet initiated by foreign agencies, for foreign crimes or with regard to other activities that may be perfectly legal in Canada.

Furthermore, it is my understanding that the Council of Europe Convention has not yet been ratified by Canada. Therefore, it would seem that whatever legal obligation is being asserted to implement its provisions is in fact non-existent.

Very frankly, if the Council of Europe *Convention on Cyber-Crime* requires intruding on the privacy rights of Canadians to an extent that cannot be justified on its own merits and that is inconsistent with our Canadian values and Canadian rights, then this *Convention* should not be ratified by the Government of Canada.

Turning to the specifics of the consultation paper, the lack of detail makes it difficult to establish exactly what is being proposed, although the overall intent, and the threat to privacy, appear clear. Accordingly, I will confine my remarks to the general proposals as outlined in the consultation paper.

Technical intercept capability

Notwithstanding the lack of credible evidence of a serious problem, I recognize that new information and communications technologies may pose a challenge to conventional interception and surveillance techniques. I accept that there may be a need to require telecommunications companies to provide a basic intercept and surveillance capability.

But what is done must be consistent with the consultation's paper insistence that the intent is simply to maintain the status quo by ensuring that existing state powers can effectively be applied to new methods of communication. This means that law enforcement and national security agencies should have the same ability to intercept and monitor e-mail and cellular telephone communications, with the same kind of judicial authorization based on the same criteria, as is now the case with regard to letter mail and conventional telephone communications.

Therefore, it may be reasonable in principle to enhance the current technical intercept capability with regard to e-mail and cellular telephone communications. But because many critical details are lacking in the consultation paper, I must reserve final judgment in this regard pending a better understanding of how the intercepts are to be carried out, by whom and for what purposes and the evidentiary thresholds, oversight controls and safeguards that will be required.

Retention and preservation orders

It is good that the consultation paper does not contemplate general retention orders for Internet and cellular telephone data. Requiring all service providers, or even individual providers, to retain data on all subscribers would be an outrageous invasion of privacy. We would not accept a proposal that law enforcement and national security agencies should be able to photocopy the mail of all Canadians or record all telephone calls just in case they may want to look at the mail or listen to the calls at some time in the future. A general retention order would be equally offensive to privacy.

I would strongly urge the government to resist any suggestions that general retention requirements be part of the lawful access initiative.

However, the consultation paper does propose the creation of a "data-preservation order" to act "as an expedited judicial order that requires service providers ... to store and save existing data that is specific to a transaction or client." The purpose of such an order is to ensure that communication service providers, as custodians of communications data, do not delete subscriber-specific information until such time as they are served with a search warrant or production order.

Preservation orders are just as dangerous and inappropriate, from a privacy point of view, as retention orders. As the consultation paper indicates, the concept of a preservation order does not exist in Canadian law. This negates the argument that this type of authority is necessary to "maintain" existing lawful access capability.

Preservation orders would enable law enforcement and national security authorities to require wireless telephone services and internet service providers to preserve detailed records of every telephone number we called, every Web site we visited, every page of that Web site we read, what we searched for and downloaded.

The consultation paper does not make it clear what level of proof of suspected wrongdoing would have to be presented to a judge in order to apply for, and serve, such an order on communication providers. Indeed, in some circumstances, no judicial involvement at all would be required; law enforcement or national security authorities themselves would simply be able to issue a preservation order.

The dangers inherent in this become even clearer when we consider that preservation orders could be served on ISPs to require them to retain the *content* of their subscribers' correspondence passing through their networks. That is, a preservation order could very well become a backdoor way to conduct interceptions, via a third party, without any of the judicial safeguards and remedies associated with interception warrants.

Nothing in the consultation paper denies that communications content might be captured in this manner. Indeed, another proposal in the paper suggests that communications content, such as in e-mail messages, when "preserved" and stored in recorded form, is arguably subject to a search warrant which is considerably less onerous to obtain.

The privacy implications of preservation orders are further compounded by the involvement of neutral third parties, i.e., the communication service provider, with all that this implies for data security and the potential for unlawful access by hackers and others.

Production orders

The consultation paper proposes the use of "production orders" to compel the custodian of documents to deliver or make them available to law enforcement officials within a specified period of time. Except for a very narrow type of production/collection order, there are currently no production orders provided for in the *Criminal Code*. Two different production orders are contemplated. Each applies to different types of information:

- A "general production order" would function in a similar manner to a search warrant. A major difference is that the physical presence of a law enforcement officer to conduct the search is not required.
- A "specific production order" would apply to "telecommunications associated data" or "traffic data" which is, arguably, subject to a lower expectation of privacy and thus a lower judicial standard for law enforcement/national security access.
- The paper also asks whether there is a need for a second type of specific production order that would apply to customer name and address and service provider information. (I will deal with this issue separately below.)

Again, the paper does not make the case for production orders—the need has not been demonstrated.

More specifically, I question the assumption in the paper that "telecommunications associated data" necessarily involves a lower expectation of privacy. The paper assumes that the traffic data generated by wireless telephone service, e-mails, or using the Internet is analogous to a record of the telephone numbers called or received from a particular number.

In the world of wireless telephony, "traffic data" also includes a record of the location of the cell phone in question as it moves about from cell to cell. For this reason, the traffic data generated by wireless calls is far more personal and revealing.

In the Internet world, traffic data would encompass the e-mail addresses on all correspondence to and from the subscriber, a record of date, time, and size of message as well as other pertinent (but unnamed) transmission details but excluding message subject and content.

And, as previously noted, Internet "traffic data" also encompasses a record of every login session, every web page visited and read, every search term entered, every file downloaded, every purchase made, and so forth—in short, virtually the entirety of one's online "session" but excluding the content of email messages.

Although the proposals outlined in the consultation paper purport to adapt or maintain law enforcement access to communications data, it is clear that this new instrument will go far beyond accessing a simple record of numbers called or received to include very intimate details and a much larger profile of our activities, thoughts, preferences, and lifestyle.

For this reason, I take issue with the assertion that this kind of data would or should be subject to the same (lower) expectation of privacy as the information generated by wireline telephone calls. What is contemplated here is an enormous expansion of access to a large and growing reservoir of data created by communications subscribers.

Given all these considerations, I am not persuaded as to the need for, nor the acceptability of, creating new instruments in the form of retention orders and production orders.

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.

The two-step process that is proposed - allowing law enforcement and national security authorities to obtain first a preservation order and then a production order – also itself carries a risk of eroding the current standards that must be met when agents of the state seek judicial authorization to invade communications privacy.

If a judge is asked only to authorize an order to "preserve" communications data, with the issue of actually "producing" that information into the hands of authorities being left for later judicial determination in a subsequent proceeding, he or she may be less inclined to insist on a high degree of satisfaction that this order is actually necessary. And, likewise, the second judge who is asked to order the actual production of the data may be more inclined to assume that the appropriateness of the whole intrusion must already have been demonstrated to the judge who approved the original retention order.

My view is that if the police or security services want to examine the online or wireless communications of any individual whom they suspect of serious wrong-doing, they should only be able to do so in the same manner that now exists with regard to other forms of communication. They should be required to obtain a judicial order, based on the same standard of proof as applies to other forms of communication, authorizing them to intercept that individual's online or wireless communications.

There is no doubt that this would be more onerous, more time-consuming and more labour-intensive than the retention order/production order technique that is proposed. But that is precisely the point: Invading the privacy of Canadians to an unprecedented extent should not be made so convenient or so easy as to encourage the carrying out of such activities on a wholesale basis rather than only in the most serious and unavoidable circumstances.

Customer name and address and service provider information

The consultation paper notes that with the deregulation of the telecommunications market, law enforcement/national security agencies are experiencing difficulties in identifying the local service provider associated with a given telephone number. The paper also refers to problems obtaining customer name and address information.

The paper suggests that it might be appropriate to create a national database containing customer name and address and service provider information for all Canadian telephone subscribers—as recommended by the Canadian Association of Chiefs of Police.

I cannot support the creation of such a database. Yes, it would make it easier for law enforcement/national security agencies to obtain customer name and address and service provider information, but the difficulties involved in obtaining this information can hardly be insurmountable. Furthermore, these difficulties serve a purpose—they force law enforcement/national security agencies to think twice before seeking to obtain this information.

The consultation paper appears to endorse a view that the name and address of an individual with a given telephone number carries such a low expectation of privacy that access to it by law enforcement authorities should be a routine procedural matter. I take issue with any assertion that one's name and address, when associated with a unique identifier like a telephone number, is somehow unworthy of privacy protection.

In consequence, I see no compelling reason to change current law and practice regarding access to this information.

Carrying this idea a step further, the consultation paper floats the possibility of all service providers being obliged by law to collect and verify the identity and address of all subscribers. This raises the spectre of convenience store clerks demanding and recording—and then transmitting—people's sensitive personal information, such as driver's license and credit card numbers, as a condition of purchasing pre-paid phones or phone cards. This would be a gross invasion of privacy.

I am likewise opposed to the idea of creating a centralized national database registry of Internet subscribers. If this were established, as has been proposed for the telephone database noted above, law enforcement authorities could automatically and routinely trace an Internet Protocol address back to the registered user, circumventing the normal due process of

requesting this information from each ISP on a case-by-case basis. Such a project, if carried out, would effectively obliterate any expectation of privacy and anonymity on the Internet.

Conclusion

As I have indicated, the consultation paper does not demonstrate why these measures are necessary. This is all the more troubling because the measures being contemplated go far beyond simply maintaining existing capabilities and authorities.

On this issue, my position is simple. I do not see any reason why e-mails should be subject to a lower standard of protection than telephone calls or letters. And I do not see why Internet browsing should be subject to a lower standard of protection than book purchasing or researching in a reference library. Canadians should not be subject to greater monitoring or scrutiny just because they choose to use new communications technologies.

In a free and democratic society like Canada, the interception and monitoring of private communications carries extraordinarily strong symbolic and psychological implications, in addition to the obvious practical ones. Canadians are entitled to feel confident that their communications and on-line activities will not be arbitrarily intercepted or scrutinized.

Yours sincerely,

(Original signed by)

George Radwanski
Privacy Commissioner of Canada

