LAWFUL ACCESS QUESTIONS AND ANSWERS
Updated November 2009

Following are answers to the most common questions arising from the CACP's position on lawful access.

Question #1:

Are the police seeking the ability to randomly eavesdrop on the telephone conversations and Internet activities of Canadians?

Response

Absolutely not. Even if it were technically feasible to do so (which it is not) it is presently, and will always be illegal for the police to indiscriminately eavesdrop on people. Strict procedural safeguards are in place that ensure the actions of the police are scrutinized. For example, before an interception can take place, strict statutory criteria must be met. The police must demonstrate to a judicial authority that these strict conditions have been satisfied before an interception order will be granted. An authorization to conduct an intercept can never permit the indiscriminate eavesdropping on anyone at anytime.

Question #2

If judicial authority must be obtained before the police can intercept communications, and if this requirement will not change, what more are the police asking for in terms of lawful access?

Response

Police requests related to lawful access falls into three general categories:

1. additional legal procedures that will facilitate the collection of evidence with respect to serious crimes. At the present time, evidence of serious crimes such as child pornography, Internet child luring for sexual exploitation, membership in criminal organizations and Internet fraud, is being lost due to the absence of adequate legal procedures to facilitate the collection of important evidence. The requested procedures would be consistent with the judicial authorization system that is presently in place in other legal procedures.
2. technological changes are required to ensure the police have the capability of physically intercepting criminal communications, regardless of the technology being used. Communication service providers (e.g., telephone companies, Internet service providers) continue to roll out new technologies that inadvertently prevent the police from conducting lawful access operations. We are asking that communication service providers be required to build intercept solutions into new technologies as they are developed.

3. laws that will resolve the serious issues related to the cost of intercept operations. The policing community acknowledges that intercept operations are expensive for both police agencies as well as communication service providers. It is our position that attempting to impose an arbitrary, non-negotiable fee with respect to the execution of a court order brings the administration of justice into disrepute. Further, the imposition of such fees will limit the effectiveness of law enforcement as investigations will become dependent on a given police agency's ability to pay.

We propose the following as possible options to address the issue of costs:

1. provide tax credits for communication service providers
2. establish a small public safety tariff that would appear on customer invoices (akin to the 911 fee)
3. provide a federal funding pool from which the costs incurred by telecommunications service providers can be recovered.

Question #3

Is the policing community simply over-reacting to the threat of terrorism?

Response

No. The lawful access related requests of the policing community have nothing to do with terrorism. The CACP is on record for asking for the modernization of lawful access laws since 1997. Present concerns with respect to terrorism are an unhappy coincidence that was not anticipated by the policing community.

Question #4

Is the lawful access initiative tied to other Government of Canada proposals such as the issuance of identity cards or the mandatory retention of commercial passenger lists for police examination?

Response

No. These initiatives have nothing to do with the lawful access issue and must be scrutinized on their own merits. The objective of the lawful access initiative is to update law enforcement's ability to conduct lawful interception as well as take into account new and emerging technologies as well as the effects of a deregulated communications industry

Question $5

Will the new powers for police to intercept personal communications permit police to go on fishing expeditions into private communications of citizens – to randomly go through people's Internet and email records trolling for things?

Response

The proposed legislation does not provide police with new powers for trolling randomly through peoples' private communications. It updates the Criminal Code to include language that reflects modern technologies and provides court orders that are appropriate to these technologies.

Question #6

Will the new legislation allow police to go on fishing expeditions that are unsupported by evidence of a crime or court oversight?

Response

Court oversight will still be required on all of the new surveillance or intercept provisions. Court oversight will not be required with the Internet Service Providers (ISPs) are asked to turn over customer name and address, however the courts have already determined there is no expectation of privacy with this information. Court oversight is also not required for policing requesting preservation of information, however judicial authorization is required for police to extend data preservation or obtain the preserved data.

Question #7

When will warrants be required to intercept personal electronic communications?

Response

Warrants will be required to intercept personal electronic communications. Warrants will not be required to obtain customer name and address information, a policy position supported by case cal. The police will require reasonable grounds to believe a crime has been or will be committed. There are some inconsistencies within Canada in regards to disclosure of subscriber information. Some telecommunication service providers/ISPs currently provide police the information without warrant, yet others require a warrant. In some cases they take this position because they are not sure whether they are allowed to disclose the information voluntarily. The legislation simply clarifies the law.

Question #8

Will police be able to remotely track private citizens through their cell phones and Blackberries?

Response

Amendments would allow police to apply for tracking warrants which would permit them to remotely activate existing tracking devices that are found in certain types of technologies such as cell phones and tracking devices in some cars. To obtain a warrant to track an individual the police would have to show there are reasonable grounds to believe that an offence has been or will be committed, and that tracking the person would assist with the investigation.

Question #9

ISPs will be forced to install monitoring technology to keep track of their users' online activities. Will that give the government and police unprecedented access to all my electronic communications and personal information?

Response

Interception and surveillance will continue to require court oversight.

Question #10

Will small ISPs be exempt from the requirement for intercept capability? Won't criminals then just turn to smaller service providers?

Response

True, criminals may turn to small service providers, but currently they also use service providers that turn over CNA without a warrant. Small ISPs will be granted a three year exemption on this requirement.

Question #11

What are the cost implications, and will costs just be passed on the consumer?

Response

The need for intercept capability may outweigh the objection that costs will be passed on to the consumer.

Question #12

Is this legislation required? There is no evidence of the need for these changes and it raises real concern for potential abuse.

Response

The Criminal Code is so outdated that we cannot ratify international treaties that would help us with international cybercrime investigations because we don't have the ability to

ensure that electronic evidence is preserved while investigators in other countries obtain the necessary authorities to obtain the data.

There is no obligation for service providers to not delete data that may be relevant to a criminal investigation. Data can quickly become lost. The ability to make requests for search warrants or production orders through the courts is included in the legislation. Current production orders are restricted to data associated with telephones only. The legislation provides for disclosure of enough transmission data to trace all service providers involved in the transmission of specific data. It does not include the substance of the communication.

The ability to obtain CNA information on an urgent basis is critical for police investigations. Police must be able to match IP addresses with an actual location to conduct investigations CNA information in a timely fashion is a critical step in this process.

Question #13

Is the legislation too far reaching, affecting all of the good people who use new technologies in order to catch a few criminals?

Response

The Internet has changed how crimes are committed, and some, such as Internet luring and on-line real time images of ongoing child sexual abuse require new tools for the police to respond quickly to locate the offender, prevent further abuse and preserve evidence. Also recognize that organized crime groups use new technologies for fraud, money laundering etc. Tools to preserve data as evidence and to participate in international investigations are required to effectively address these crimes.

Question #14

Is this legislation typical of the Conservative government's move toward a police state?

Response

Canada has been under pressure for a decade to update its legislation to be consistent with new technologies and to be able to investigate sophisticated online crimes such as market fraud and child pornography and to take part effectively in international cyber-crime investigations. The current lawful access package is essentially the same as that proposed by the former Liberal government This is not a partisan issue.