



Backgrounder

BACKGROUNDER

Technical Assistance for Law Enforcement in the 21st Century Act

INTERCEPT COMPONENT

The interception of communications is essential for investigating and prosecuting serious crime and combating terrorism. Police forces and the Canadian Security Intelligence Service (CSIS) require lawful access to communications in a number of contexts, including investigations into child sexual abuse, organized crime, drug trafficking, and terrorism.

The *Technical Assistance for Law Enforcement in the 21st Century Act* will not provide law enforcement or CSIS with any new interception powers, nor will it change or expand existing interception authorities in any way. Rather, it will address the challenges posed by modern technologies that did not exist when the legal framework for interception was designed nearly 40 years ago. Police forces and CSIS will continue to require warrants for interception. This legislation will simply ensure that when warrants are issued, a technical solution is available so that police forces and CSIS can actually intercept communications.

Canada currently has no legal requirement for companies to build interception capability into telecommunications networks. As a result, we now have situations where judicial authorization is granted (a warrant is issued), but cannot be effected because the service provider's network is not intercept capable. Criminals and terrorists are aware of interception "safe havens" and exploit them to continue their criminal activities undetected. As new telecommunications services and products are being rolled out every day, police forces and CSIS continue to fall behind increasingly sophisticated criminal and terrorist groups. There are far too many instances where police forces and CSIS cannot execute judicially authorized interceptions to protect Canadians' safety, simply because of a lack of intercept capability on telecommunications networks.

A technical solution will now be available for police forces and CSIS to execute judicially authorized warrants.

The proposal will require companies to pay for intercept capability in certain new equipment and software, while the Government will provide reasonable compensation when retrofits to existing networks are needed – this is a shared response to a problem that directly affects the safety of Canadians.

Along with sharing the cost of fixing this problem, we have built flexibility into the legislation. For example:

- o A number of entities (such as banks, private networks, and charities) are excluded from the legislation's requirements, and will not be required to have intercept capability.
- o A three-year exemption will be granted to "small" service providers (those with less than 100,000 subscribers) from certain requirements deemed too costly for them at this time. After the three years, these companies will be expected to fully comply with the requirements of the legislation.
- o Upon approval by the Government, exemptions may be granted to service providers for two-year periods, with conditions, to permit innovative technologies to be brought to the marketplace prior to being fully compliant with the requirements of the Act. This will allow service providers to remain competitive in the global marketplace, while developing intercept solutions for these new technologies.
- o Service providers will also be free to select the most cost-effective intercept solutions available, and will not be tied to government-determined standards or equipment.

This flexible and gradual approach will avoid placing an undue burden on industry, while at the same time ensuring that telecommunications service providers build and maintain interception capability on a going-forward basis. In doing so, this legislation strikes the right balance between the needs of police forces and CSIS, the safety and security of Canadians, and the competitiveness of industry.

Nothing in this legislation will diminish the considerable legal protections currently afforded to Canadians with respect to privacy or freedom from unreasonable search and seizure.

SUBSCRIBER INFORMATION COMPONENT

Police forces and CSIS also require timely access to basic subscriber information as it is an essential tool for fighting crime and terrorism. Subscriber information refers to basic identifiers such as name, address, telephone number and Internet Protocol (IP) address, e-mail address, service provider identification and certain cell phone identifiers. These basic identifiers are often crucial in the early stages of an investigation, and without this basic information, police forces and CSIS often reach a dead-end as they are unable to obtain sufficient information to pursue an investigative lead or obtain a warrant.

Currently, there is no legislation specifically designed to require the provision of this information to police forces and CSIS in a timely fashion. As a result, the practices of releasing this information to police forces and CSIS vary across the country: some service providers release this information to law enforcement immediately upon request; others provide it at their convenience, often following considerable delays; while others insist on law enforcement obtaining search warrants before the information is disclosed. This lack of national consistency and clarity can delay or block investigations.

A consistent, balanced, well-regulated and accountable solution is needed for law enforcement and CSIS to obtain basic subscriber information in order to protect the public's safety and security, while safeguarding individual privacy interests. The *Act* will accomplish this by compelling all service providers to release this information and creating an administrative model that provides for a reporting regime which ensures accountability by including consisting of a number of new, privacy-related safeguards. Safeguards include such things as the designation of a limited number of law enforcement and CSIS officials who can request information, record keeping, and both internal audits and external oversight.

This legislation provides law enforcement and CSIS with the updated tools needed in the face of rapidly changing technology, while providing maximum flexibility for industry, and creating rigorous safeguards to protect privacy. In doing so, this legislation strikes an appropriate balance between the needs of law enforcement and CSIS, the competitiveness of industry, and the privacy rights of Canadians.