National Security Consultation
Public Safety Canada
269 Laurier Ave. West
Ottawa, ON K1A 0P8

ITAC RESPONSE TO FEDERAL CONSULTATION ON NATIONAL SECURITY

The Information Technology Association of Canada (ITAC) appreciates the opportunity to participate in Public Safety Canada's review of Canada's National Security framework. ITAC is the authoritative national voice of Canada's $170 billion information and communications technology (ICT) industry. Canada's 36,000 ICT firms, ranging from major telecoms to start up software developers, generate over 1.1 million jobs directly and indirectly. The ICT industry in Canada also creates and supplies goods and services that contribute to a more productive, competitive and innovative economy and society.

Government plays a key role in keeping communities safe. Canada's ICT industry appreciates that law enforcement needs access to digital information to bring criminals to justice and protect Canadians from terrorist threats. However, in a democratic society it is also critical that government works to strike a balance between public safety, privacy and fundamental freedoms. This can best be accomplished by adopting a framework for addressing national security issues that respects the rule of law, ensures proportionality and acknowledges the importance of transparency and accountability.

Prior to pursing new digital surveillance powers, it is important the government build a consensus across Canadian society on the right balance between security and privacy as well as the appropriate transparency and oversight mechanisms governing the exercise of state power. The Supreme Court of Canada has provided helpful guidance. In *R. v. Oakes*, the Court set out a four-part test for determining whether a violation of a right protected by the *Charter of Rights and Freedoms* is nonetheless justifiable in a free and democratic society. Known as the "*Oakes test*", a violation of a protected right is justifiable only if there is:

1. *Necessity* (i.e, a clearly defined necessity for the use of the measure);
2. *Proportionality* (i.e., the measure must be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the privacy (or any other rights) of the individual being curtailed);
3. *Effectiveness* (i.e., empirical evidence that the measure is effective); and
4. *Minimal intrusiveness* (i.e., the measure must be the least invasive alternative available).

By applying this framework to national security issues, the government will both be respecting our constitution and maintaining the trust of Canadians.

5090 Explorer Drive, Suite 510, **Mississauga**, Ontario, Canada L4W 4T9
Phone 905-602-8345, Fax 905-602-8346
220 Laurier Ave. West, Suite 1120, **Ottawa**, Ontario, Canada K1P 5Z9
Phone 613-238-4822, Fax 613-238-7967

ICT businesses, including ITAC's members, are important stakeholders in building a consensus on national security issues. Many ICT businesses find themselves in the unenviable position as intermediary between end users of their products, on the one hand, and law enforcement and national security agencies, on the other. This means that ICT businesses must work hard to respect privacy and build the trust of their customers, while also satisfying their legal obligations concerning the preservation and disclosure to law enforcement of customer information.

ICT businesses connect Canadians, improve their productivity and secure their data. Requiring surveillance capabilities or backdoors to support law enforcement could undermine technology used every day by millions of law abiding Canadians – potentially putting their privacy and security at risk.

Surveillance capabilities or backdoor requirements may also undermine Canada's innovation economy. Our assessment takes into account that:

- Consumers and businesses will only use technology they trust;
- Canada-specific technical requirements will make it more difficult for businesses, particularly small and medium-sized enterprises, to compete in the global marketplace and more costly for Canadian consumers and businesses to adopt productivity enhancing tools;
- Canada may lose one of its competitive advantages in ICT (that is, its status as a jurisdiction in which personal data from the European Union may be processed); and
- Surveillance requirements will significantly distract ICT businesses from their core objective of continuous innovation in a hyper-competitive marketplace.

The considerable financial costs to ICT businesses of new surveillance powers also needs to be highlighted. Many of the national security tools described in the government's Green Paper would, if implemented, require significant capital investments by ICT businesses, as well as material ongoing expenditures. These costs, as law enforcement expenditures, are appropriately borne by the state. ICT businesses should be fully compensated for any related capital or ongoing costs they incur to comply with government-imposed law enforcement requirements. Additionally, ICT businesses should have an efficient and effective means of seeking and receiving this compensation.

Specific Consultation Areas:

Access to Basic Subscriber Information

The decision of the Supreme Court of Canada in *R. v. Spencer* makes a strong statement about the need for judicial oversight where there is a reasonable expectation of privacy. This includes online interactions where users would otherwise be anonymous.

5090 Explorer Drive, Suite 510, **Mississauga**, Ontario, Canada L4W 4T9
Phone 905-602-8345, Fax 905-602-8346

220 Laurier Ave. West, Suite 1120, **Ottawa**, Ontario, Canada K1P 5Z9
Phone 613-238-4822, Fax 613-238-7967

Presently, law enforcement agencies are advocating for the removal of the *Spencer* requirement for judicial oversight to improve the efficiency of accessing BSI. Pitting effective oversight against efficient administration of the BSI process is a false dichotomy. Rather than weakening oversight or circumventing the guidance of the Supreme Court of Canada, the government should investigate what is inefficient or inadequate in the current process for accessing BSI and seek to address these challenges.

Presently there are a number of administrative steps the government could take to improve the efficiency, predictability and timeliness of the existing court order process. For instance, different law enforcement bodies, from the RCMP to local police detachments, submit orders using different forms, definitions and delivery methods. This causes significant challenges for industry to return a timely and consistent response. The federal government should work with industry and law enforcement bodies across Canada to develop standardized templates and definitions that improve the consistency and predictability of BSI court orders. These should include:

- A standardized court order form for use across all police services.
- Clear and narrowly defined terms for the information sought.
- Clear rules designed to avoid police "fishing expeditions" that could contravene judicial requirements and privacy laws.

As the government considers its options for dealing with BSI, care should be taken to avoid the risk of scope creep. As encryption and similar technologies limit law enforcement's ability to access digital information, there may be a desire to expand the types of subscriber information considered "basic" by, for example, including data like social network or email account details. Where this information is subject to a reasonable expectation of privacy, the safeguards identified in the *Spencer* decision will need to be respected.

Intercept Capability

Requiring communication service providers to build interception capabilities into their networks would create significant challenges for ICT businesses. Interception has been discussed and debated for the past 15 years, including as recently as 2012 when the previous federal government decided not to pursue such a requirement.

If the government were to propose that an interception capability be created now, it would be critical that the government identify how the related costs, including risks to Canadians in respect of privacy and network security, are justified. In part, this would require that the government demonstrate the effectiveness of interception. However, in light of the prevalence of end-to-end encryption and availability of online services offered from outside of Canada, proving effectiveness may be difficult. At most, interception capabilities may only yield evidence in respect of the least sophisticated criminals, with any related benefits being offset by the risk of surveillance backdoors being exploited by hackers and other criminals, including foreign actors.

5090 Explorer Drive, Suite 510, **Mississauga**, Ontario, Canada L4W 4T9
Phone 905-602-8345, Fax 905-602-8346

220 Laurier Ave. West, Suite 1120, **Ottawa**, Ontario, Canada K1P 5Z9
Phone 613-238-4822, Fax 613-238-7967

While there are emerging technologies that can dis-intermediate telecom companies (e.g. Stingray), these technologies can negatively impact telecom networks (e.g. 911 access) as well as create additional privacy-related vulnerabilities. Prior to introducing these technologies, law enforcement should work with industry and privacy experts to fully understand impacts and address potential risks.

If any expansion in intercept powers is pursued, the government needs to ensure they do not inadvertently discourage innovation and undermine Canada's reputation as a trustworthy technology jurisdiction. For instance, moving data and business functions to the cloud can offer material productivity benefits for Canadian firms. If interception capabilities were to put data stored in the cloud at risk, adoption of cloud solutions may be suppressed.

Encryption

Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better and communications between loved ones. Governments, including the federal government, fund the creation and deployment of sophisticated encryption technology. Encryption, in short, protects people.

The Green Paper raises the question of how to balance encryption that protects the security of individuals with the needs of law enforcement to access information for investigations. From an industry perspective, there is no magic bullet for ensuring security and privacy while giving law enforcement easy access to all the information it wants. Reducing the strength of encryption or requiring "backdoors" that could be exploited by cyber criminals puts everyone's security and privacy at risk. At a time when initiatives like the Public Safety Canada's *Get Cyber Safe* campaign are working to increase Canadians' cyber security protection, actions to weaken encryption would directly undermine these efforts. The reality is that encryption technologies today are readily available around the world. If encryption is weakened or outlawed, criminals will continue to have access to it and it is law-abiding citizens who will suffer. That is a bad outcome.

Any requirement for backdoors would also seriously undermine Canada's growing cyber security industry which enjoys a strong international reputation. It would make it more challenging for Canadian firms to do business internationally, and discourage multinationals from conducting cyber security research and development work in Canada.

Data Retention

Any suggestion of the government mandating bulk storage of telecommunication information for all users would be a significant departure from existing practices and would raise serious questions about Canadian's privacy rights. Additionally, the costs of mass data retention would be significant.

5090 Explorer Drive, Suite 510, **Mississauga**, Ontario, Canada L4W 4T9
Phone 905-602-8345, Fax 905-602-8346

220 Laurier Ave. West, Suite 1120, **Ottawa**, Ontario, Canada K1P 5Z9
Phone 613-238-4822, Fax 613-238-7967

If the government moves forward with a mass data retention requirement, it would need to be prepared to cover all related costs incurred by ICT businesses and work with industry to develop an effective framework for compensation, including the recovery of damages in respect of cyber security attacks involving data that the ICT business would have deleted but for the legal requirement to retain it.

Conclusion

There is no doubt that, along with a myriad of benefits, technology has created new platforms for criminal or terrorist activity. While it is clear that law enforcement approaches to investigating and preventing crime need to adapt to these new platforms, it is critical that the government ensure that any changes to law enforcement powers do not undermine Canada's innovation economy or the privacy or fundamental freedom of Canadians. ITAC and our members look forward to continuing discussions with government on these essential issues for our country. We would be pleased to provide specific details on any of the areas discussed above at the government's convenience.

For additional information please contact David Messer, Senior Director – Policy, ITAC at dmesser@itac.ca