ENCRYPTION AND LAW ENFORCEMENT

ISSUE:

To provide the Minister of Public Safety and Emergency Preparedness with information about the impacts of police being unable to obtain judicially authorized digital evidence due to the encryption of this evidence, whether it is data-in-motion or data-at-rest, in relation to the joint meeting of the Five Country Ministerial and Quintet of Attorneys General on February 16, 2016, in Washington, D.C., "Session 3: Cyber – Encryption and How to Engage with ISPs."

Introduction – "Going Dark"

Digital technologies and electronic communications have transformed Canadian society and facilitated online commerce and trade, among other economic and societal benefits. Advances in technology, such as encryption, have also helped to secure Canada's information technology (IT) systems and networks, which provide tangible cyber security, privacy, and public safety outcomes. These benefits, however, are accompanied by troubling public and community safety risks.

Police in Canada face technological, regulatory, and/or jurisdictional barriers to obtaining judicially authorized digital evidence. Taken together, these challenges are referred to as the "going dark" problem. Primarily, these barriers relate to:

- The lack of intercept capabilities in some of Canada's Internet and telecommunications/ cellular networks;
- The use of encryption by criminal targets to protect their communications (data-in-motion) or stored data (data-at-rest);
- A lack of adequate data retention regulations or standards (e.g. communications service providers destroying potential digital evidence within hours or days, before investigators can obtain it); and,
- Jurisdictional issues, such as when data is stored outside of Canada, thereby necessitating a mutual legal assistance (MLA) request where there is one in place.

These barriers are not necessarily mutually exclusive. For example, police investigators may have the technological capability to intercept real-time private communications (data-in-motion) under a *Criminal Code* PART VI judicial authorization, but may in turn be unable to decrypt and read these data. Encryption can also be applied to data-at-rest, such as data on a smart phone or in the cloud.

Barriers to obtaining digital evidence hamper police investigations, and police services are the only organizations in Canada that can pursue criminals. Police do so by gathering criminal intelligence and conducting investigations that ultimately lead to criminal law proceedings and prosecutions in Canada or abroad.

Encryption

Encryption is a neutral technology that can be applied to data-in-motion or data-at-rest. Data-in-motion can have layers of encryption applied to it by the end user, third party applications, and/or by telecommunications service providers (TSPs) during the transit over their networks. Some encryption technologies use a single, long-term master encryption key, which allows the holder of this master key to decrypt any data which was ever encrypted with that key. Should the master key be compromised, all of its users are put at risk. As a result of this vulnerability, advancements in encryption technology have moved away from relying on a single master key. For example, forward secrecy involves generating and then deleting a unique key for each individual transaction, so that stealing the decryption key used by a server cannot compromise earlier or later communications. As these types of technologies become ubiquitous, the challenges faced by police will become all the more acute.

Encryption challenges also apply to the court-ordered production of historical data, such as e-mail, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Data from these devices and modes of communication may have layers of encryption that make them unreadable.

Encryption technologies are intended to increase privacy and security, but create a black hole for law enforcement when a method for decrypting or otherwise removing the encryption is unavailable. In some cases, major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level, and therefore these companies cannot provide technical assistance to government agencies to decrypt or otherwise remove encrypted data found on lawfully seized devices. At present, there is no Canadian legislation that compels TSPs and IT manufacturers to remove their added encryption in response to a court order, even where it is readily possible for them to do so in the context of a judicially authorized interception of data-in-motion or court order for data-at-rest.

STRATEGIC CONSIDERATIONS:

The "going dark" digital evidence challenges, including encryption, continue to undermine criminal investigations in Canada and internationally. This problem is likely to become even more pronounced as technology continues to develop at an exponential rate.

Digital evidence challenges are often raised by international partners (e.g. U.S. Federal Bureau of Investigation [FBI], UK National Crime Agency [NCA]) at meetings of the Five Eyes Law Enforcement Group (FELEG)[1] and public fora, and Canada is largely behind its close allies in terms of addressing some of these issues. In late 2015, with RCMP support the FBI proposed the creation of a Going Dark FELEG Forum to work through many policy issues and technical challenges of Going Dark, while closely coordinating with the Quintet of Attorney Generals.

Canada's allies have by no means resolved how to police the Internet or solve the "going dark" problem, but they are further ahead in advancing reform measures to address some of these issues, or at minimum, advancing a more complete and well-rounded conversation with all

[1] FELEG: Chiefs of the Australian Federal Police, New Zealand Police; NCA; RCMP; and, the U.S. FBI, Homeland Security Investigations, and Secret Service.

stakeholders. The following table provides an overview of how Canada compares.

Investigative capability	AUS	CAN	NZ	UK	USA
Legal remedies for encryption				∏	∏
Extra-territorial reach legislation to assist in accessing data stored abroad	∏		√	√	∏
"Communications service" is broadly defined (not infrastructure specific)	√		√	√	∏
Retention of communications data is required by law	√			√	
Intercept capable services are required by law (full or partial coverage)	√		√	√	√
Administrative regime for access to subscriber information	√		√	√	√
√ In place	∏ Active dialogue / in progress				
Source: Public Safety Canada and RCMP (2015)					

It will be important for the Public Safety Portfolio to reframe "lawful access" as broader "going dark" digital evidence challenges, and to address the problem in terms of its broad impact on individual Canadians, private businesses, and the delivery of Government services. Foremost, the problem must be articulated in terms of its impact on safety and the economic well-being of individuals and businesses. This will require messaging that aims to re-establish the importance of balancing community safety needs with online privacy and anonymity expectations.

The RCMP, in concert with other security and intelligence federal organizations and the Canadian Association of Chiefs of Police, continues to examine solutions to address the various "going dark" digital evidence challenges. Fundamentally, this requires two actions. The first is the creation of a new public narrative around why police need judicially authorized and timely access to online information in order to keep Canadians safe and allow businesses to prosper. This will need to be supported by evidence of the impacts on police operations of the various digital evidence challenges. The RCMP is currently in the early stages of its own quantitative and qualitative study in relation to intercept challenges and encryption and their operational impact (e.g. delays, increased costs, or fewer or lesser charges). However, it is difficult to capture cases where police did not seek judicial authorization for digital evidence due to certain barriers, and instead pursued an alternate investigative strategy (e.g. undercover work).

Second, the RCMP, Justice, and Public Safety will need to work with Five Eye partner countries to tackle this problem in a coordinated fashion, which will increase our collective clout when engaging with TSPs, industry, and privacy-related academics. This is particularly important given the challenges associated with developing a legislative or regulatory solution. Domestically, the RCMP engages with security managers from the five largest TSPs on law enforcement challenges such as those in relation to interception of judicially authorized private communications, but further outreach at a senior level in concert with Five Eyes allies would be beneficial. There are indications that certain TSPs and IT companies, such as BlackBerry, are actively supportive of law enforcement efforts vis-a-vis interception and encryption in relation to their networks or products.

RECOMMENDATION:

It is recommended that you actively support action toward further senior-level engagement of TSPs, other IT industry partners, and privacy-related academics by the Five Eyes partner countries as such.