FOR OFFICIAL USE ONLY
AU, CAN, NZ, UK, USA

Australian Government Department of Home Affairs | Department of Justice Canada | DEPARTMENT of the PRIME MINISTER and CABINET | Home Office

Five Country Ministerial

Quintet of Attorneys General

STATEMENT OF PRINCIPLES

ENCRYPTION

Pages 2 to / à 3

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

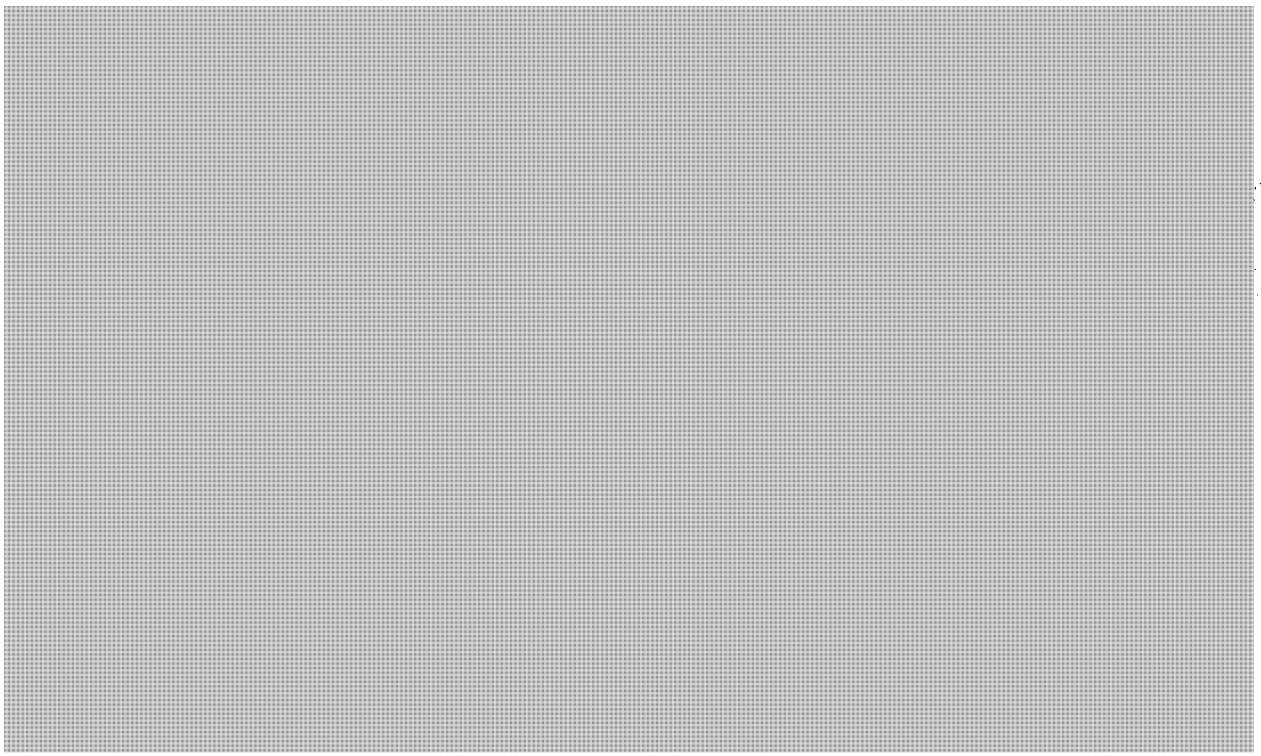
ISSUE

A draft communique has been proposed for the Five Country Ministerial meeting that includes a Statement of Principles on encryption.

CONSIDERATIONS

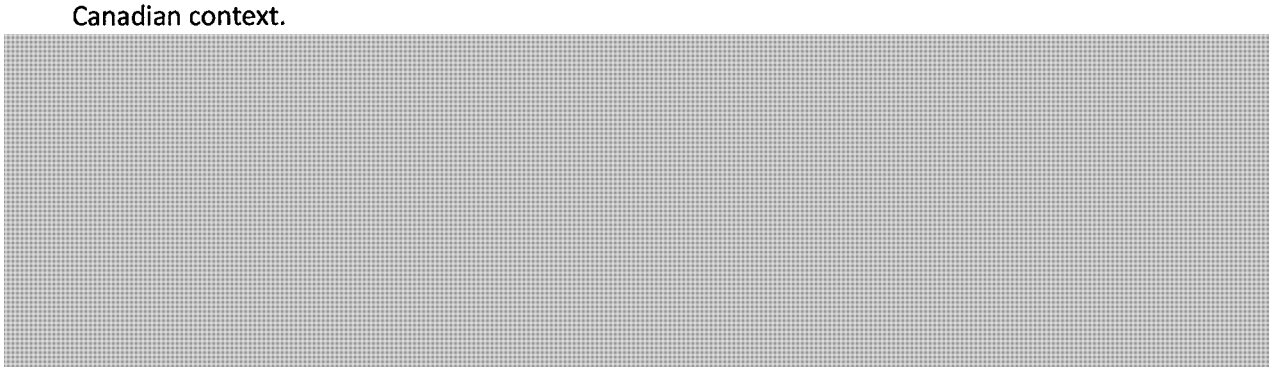
Australian position

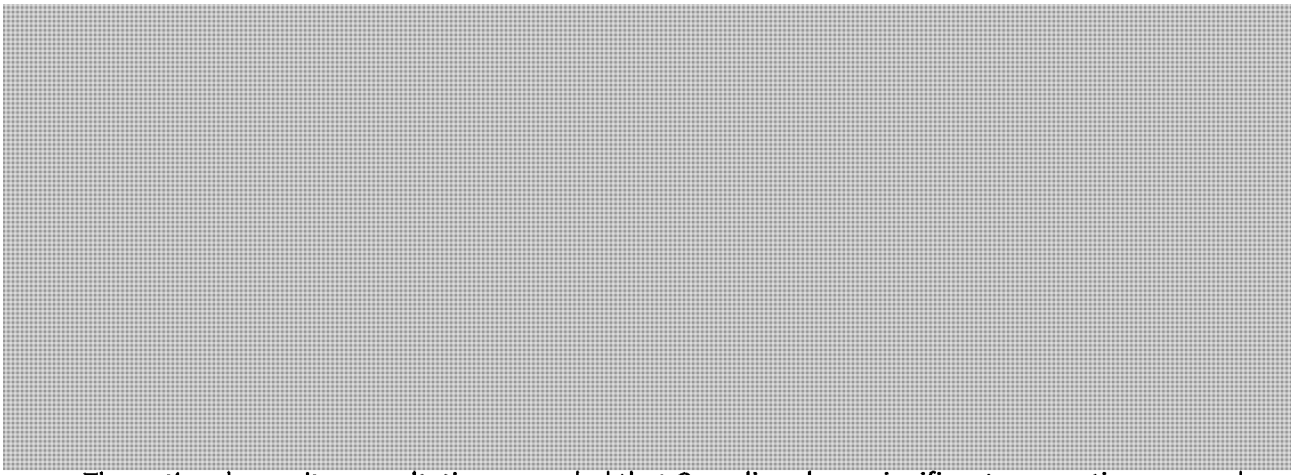
- This year, the host Australia has proposed language in the communique, Statement of Principles (**Tab A**), and scoping paper (**Tab B**) that is in line with legislation that the Australian government will be tabling shortly.



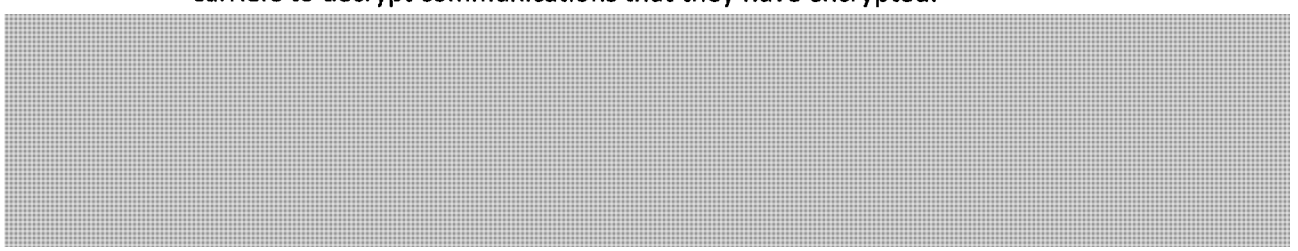
Canadian position

- Canada could support the idea that further action needs to be taken with respect to encryption, however some of the proposed language in the communique could be misinterpreted in the Canadian context.

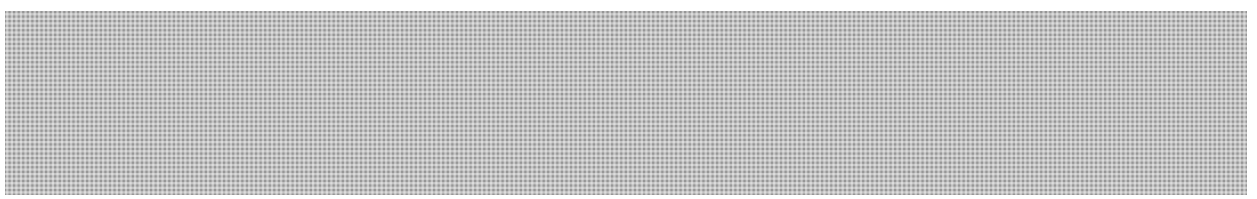




- The national security consultations revealed that Canadians have significant reservations around the idea of compelling assistance with decryption from either individuals or service providers, despite acknowledgment of the necessity of lawful interception.
- Canada's current framework for lawful access to encrypted communications (see **Tab E** for further detail) limits the scope of action that could be taken with respect to encryption. Only two tools are currently available:
    - Assistance orders, pursuant to s. 487.02 of the *Criminal Code* and s. 22.3 of the *CSIS Act*, can be used to require the assistance of any person if reasonably necessary to give effect to a warrant.
    - Standard 12 of the Solicitor General's Enforcement Standards (SGES) requires wireless carriers to decrypt communications that they have encrypted.



SUGGESTED CHANGES TO THE TEXT



- Proposed comments on the Statement of Principles are attached.

Pages 6 to / à 60

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 15(1) - Int'l

of the Access to Information

de la Loi sur l'accès à l'information

s.13(1)(a)
s.15(1) - Int'l

Comparison of legislation governing encryption across the five partners

Legislative Provisions

Overall, the various pieces of legislation contain a mix of the following provisions:

- **General Assistance:** In some cases, general purpose laws requiring companies to assist the government can be used to request or require assistance with decryption.
- **Immunity from civil liability:** Companies may not be held liable for providing law enforcement or security agencies with assistance in good faith in accordance with their lawful authorities.
- **Voluntary assistance:** Agencies may request voluntary assistance from Communication Service Providers (CSPs) to aid with investigations. Certain countries provide incentives for CSPs who comply with agency requests.
- **Technical assistance notices:** Agencies may require CSPs to provide assistance with decryption, where the CSP is already capable of doing so.
- **Technical capability notices:** Agencies may require CSPs to build new capabilities in their technology to assist with decryption.

Some legislative frameworks also include limitations on these provisions, including:

- **No new capabilities:** Providers cannot be required to build new capabilities
- **No systemic access:** Provisions specifying that providers do not need to modify the underlying service in order to ensure that readable copies of any communication can be provided

In some countries, certain obligations can apply only to specified types of service providers. For example, domestic telecommunications carriers may be subject to greater obligations than device manufacturers or online service providers.

Table 1 - Legislative provisions across the Five Countries

	General assistance	Technical assistance orders	Technical capability orders	No new capabilities	Systemic access to encrypted communications	No systemic access to encrypted communications
Canada	✓					
U.S.A.	✓					
United Kingdom		✓	✓		?	
Australia						
New Zealand		✓		✓		✓

Australia

[redacted]

United Kingdom-The Investigatory Powers (Technical Capability) Regulations 2018

The United Kingdom clearly identifies in its legislation that CSPs must provide and maintain interception capabilities so that they may assist law enforcement when faced with a warrant. This includes encrypted communications, subject to technical feasibility.

Given that there are no specific limitations in law, other than technical feasibility, it is unclear what the limits of these powers are in practice.

New Zealand-Telecommunications (Interception Capability and Security) Act 2013

New Zealand clearly identifies in its legislation that CSPs must decrypt information where they are already capable of doing so.

The legislation specifies that CSPs cannot be required to build new capabilities, or to guarantee systemic access to encrypted communications.

United States

The Unites States has no legislation specifically addressing encryption. Instead law enforcement agencies have made use of general assistance provisions, specifically the *All Writs Act*. The best known example of this occurred when the FBI attempted to compel Apple to assist in accessing an encrypted iPhone used by a perpetrator of the San Bernardino terrorist attack in 2015. Apple challenged the order in court; however, the case was never resolved as authorities found other means of accessing the device.

Legal Framework for Lawful Access

Law enforcement and national security agencies obtain judicial authorizations to intercept private communications under the *Criminal Code* and the *CSIS Act* when investigating crimes or threats to national security. However, Canada's legislative framework on lawful interception has not kept pace with technological advances of recent decades, which has created significant challenges for law enforcement in three main areas.

BSI

Basic subscriber information (BSI) consists of identifying information that corresponds to a customer's telecommunications subscription. This can include the name and contact information associated with a phone number or IP address, but does not include the contents of communications. In 2014, in *R. v. Spencer*, the Supreme Court of Canada decided that the police could not request BSI of a person in relation to his or her IP address where it would reveal intimate details of his or her anonymous online activities, except in an emergency situation or pursuant to a reasonable law. Without specific legislation designed to permit access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI since the *Spencer* decision. Instead, law enforcement agencies have had to rely on tools already available in the Criminal Code, such as general production orders and assistance orders, which were not designed for this purpose and can result in delays.

Intercept Capability

With the exception of the Solicitor-General's Enforcement Standards, which are a condition of license for wireless carriers, Canada's legal framework does not impose any obligations on telecommunications carriers to build or maintain the capability to intercept and deliver intercepts requested under lawful authority in a timely manner. To date, solutions have been developed on a voluntary basis with willing carriers, with the government largely responsible for funding these capabilities.

Encryption

Encryption converts a readable electronic message into an unreadable message, which can only be accessed by someone who holds the decryption key. Encryption is essential to secure communications on the public Internet. However, the rise in accessibility of strong encryption technology in the wake of the Snowden revelations has created significant challenges for law enforcement and security agencies. A large fraction of intercepted data is unreadable due to the layers of encryption that cannot be decrypted or otherwise removed. The only provision specifically designed to compel decryption in Canadian law is the Solicitor-General's Enforcement Standards, which are a condition of license for wireless carriers. Assistance orders, pursuant to s, 487.01 of the *Criminal Code* can also in principle be used for this purpose, although this use case has not been tested in court.