

FIVE COUNTRY
MINISTERIAL



AUSTRALIA 2018

QUINTET MEETING
of Attorneys-General

STATEMENT OF PRINCIPLES ON
ACCESS TO EVIDENCE AND
ENCRYPTION

PREAMBLE

The Governments of the United States, the United Kingdom, Canada, Australia and New Zealand are committed to personal rights and privacy, and support the role of encryption in protecting those rights. Encryption is vital to the digital economy and a secure cyberspace, and to the protection of personal, commercial and government information.

However, the increasing use and sophistication of certain encryption designs present challenges for nations in combatting serious crimes and threats to national and global security. Many of the same means of encryption that are being used to protect personal, commercial and government information are also being used by criminals, including child sex offenders, terrorists and organized crime groups to frustrate investigations and avoid detection and prosecution.

Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute. It is an established principle that appropriate government authorities should be able to seek access to otherwise private information when a court or independent authority has authorized such access based on established legal standards. The same principles have long permitted government authorities to search homes, vehicles, and personal effects with valid legal authority.

The increasing gap between the ability of law enforcement to lawfully access data and their ability to acquire and use the content of that data is a pressing international concern that requires urgent, sustained attention and informed discussion on the complexity of the issues and interests at stake. Otherwise, court decisions about legitimate access to data are increasingly rendered meaningless, threatening to undermine the systems of justice established in our democratic nations.

Each of the Five Eyes jurisdictions will consider how best to implement the principles of this statement, including with the voluntary cooperation of industry partners. Any response, be it legislative or otherwise, will adhere to requirements for proper authorization and oversight, and to the traditional requirements that access to information is underpinned by warrant or other legal process. We recognize that, in giving effect to these principles, governments may have need to engage with a range of stakeholders, consistent with their domestic environment and legal frameworks.

PRINCIPLES

The Attorneys General and Interior Ministers of the United States, the United Kingdom, Canada, Australia and New Zealand affirm the following principles in relation to encryption

1. Mutual Responsibility

Diminished access to the content of lawfully obtained data is not just an issue for Governments alone, but a mutual responsibility for all stakeholders.

Providers of information and communications technology and services - carriers, device manufacturers or over-the-top service providers -- are subject to the law, which can include requirements to assist authorities to lawfully access data, including the content of communications. Safe and secure communities benefit citizens and the companies that operate within them.

We are always willing to work with technology providers in order to meet our public safety responsibilities and ensure the ability of citizens to protect their sensitive data. Law enforcement agencies in our countries need technology providers to assist with the execution of lawful orders. Currently there are some challenges arising from the increasing use and sophistication of encryption technology in relation to which further assistance is needed.

Governments should recognize that the nature of encryption is such that there will be situations where access to information is not possible, although such situations should be rare.

2. Rule of law and due process are paramount

All governments should ensure that assistance requested from providers is underpinned by the rule of law and due process protections.

The principle that access by authorities to the information of private citizens occurs only pursuant to the rule of law and due process is fundamental to maintaining the values of our democratic society in all circumstances – whether in their homes, personal effects, devices, or communications. Access to information, subject to this principle, is critical to the ability of governments to protect our citizens by investigating threats and prosecuting crimes. This lawful access should always be subject to oversight by independent authorities and/or subject to judicial review.

3. Freedom of choice for lawful access solutions

The Governments of the Five Eyes encourage information and communications technology service providers to voluntarily establish lawful access solutions to their products and services that they create or operate in our countries. Governments should not favor a particular technology; instead, providers may create customized solutions, tailored to their individual system architectures that are capable of meeting lawful access requirements. Such solutions can be a constructive approach to current challenges.

Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions.