Encryption

Background

Encryption has gained considerable traction over the years as the importance of online content for the public, business, and governments has grown. Encryption protects the integrity of critical national infrastructure, individuals, and businesses, from malicious intrusion, including everything from telecommunications and transportation systems to financial services and the energy sector. More and more communication products and services for personal use are defaulting to the use of strong encryption to protect exchanges from being exploited.

While encryption has had several positive impacts, it has also seriously impeded law enforcement and national security agencies' ability to investigate in cyberspace, even when the agencies obtain the appropriate authorisation from a judge to intercept the communication of a suspect. This problem has been exacerbated by "user controlled end-to-end encryption", which protects data such that it can only be read either at the point of the sender or the recipient. Many mobile devices now feature full disk encryption when locked,

Encryption is a significant obstacle for the full spectrum of law enforcement and national security investigations,

As much as 67% of data that the CSIS lawfully collected in the fiscal year 2017-2018

Technology continues to trend towards more encryption. All Apple devices now employ full disk encryption by default. In March 2019, Facebook announced its "Privacy-Focused Vision for Social Networking", which is its plan to combine Facebook Messenger, WhatsApp, and Instagram into one encrypted communications platform.

Status

Without robust and timely information and evidence, the RCMP cannot investigate or intervene to halt criminal activity such as online child exploitation. CSIS ability to monitor and counter threats to national security is similarly affected by the difficulty in accessing digital data.

[redacted]

Considerations

Increasing Transparency

One of the main difficulties that impedes governmental efforts to change lawful access policies, legislation or funding is the public's lack of understanding and trust around these issues. The lack of clarity on the government's authorities and capabilities in different circumstances has led to an erosion of public trust, which has fed opposition to proposed governmental actions. Any progress on encryption will require more transparency, including strong public outreach and improved communications. It would also be essential to engage key stakeholders and gain the support of prominent voices in industry and academia.

Five Eye Discussions

Recently, Cabinet level officials have raised the subject of encryption with Canadian counterparts in bilateral meetings, and at meetings of the Five Eyes Ministers. [redacted] For the last three years, there has been a strong push among the partners for collective action to be taken on the subject. Canada's position is to support safeguarding encryption while being a proponent of mitigating its challenges through cooperation and positive relations with industry.

Next Steps

With approval, Public Safety Canada along with federal partners is proposing to:

[redacted]