DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY SPOKEN QUESTION ON NOTICE

Joint Law Enforcement

20 February 2023

QoN Number: 1

Subject: End-to-end encryption policy change. Do you have any work that you've been doing in that area that you can advise the committee on?

Asked by: Helen Polley

Question:

CHAIR: I have a couple of questions for Home Affairs in relation to end-to-end encryption policy change. Do you have any work that you've been doing in that area that you can advise the committee on?
Mr Anstee: Thank you, Chair. There are probably two aspects to update you on. For visibility of the committee, there's the distribution of policy between Attorney-General's Department and the Department of Home Affairs, as well as an update on some of the policy activities at Home Affairs. For your awareness, of the policy issues which relate to encryption, AGD leads on lawful access, electronic surveillance and child protection policy, whereas Home Affairs really leads on the cybersecurity, data security and technology security questions. In terms of an update on our policy activities at the department, we continue to find signatories to the international statement on end-to-end encryption and public safety. You may be familiar with the statement from previous committee hearings. I'm happy to share a copy with you following this hearing.

Answer:

A copy of the International Statement on End to End Encryption and Public Safety has been attached for tabling (Attachment A refers).

INTERNATIONAL STATEMENT: END-TO-END ENCRYPTION AND PUBLIC SAFETY

We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people, as stated in the 2017 resolution of the UN Human Rights Council[1]. Encryption is an existential anchor of trust in the digital world and we do not support counter-productive and dangerous approaches that would materially weaken or limit security systems.

Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children. We urge industry to address our serious concerns where encryption is applied in a way that wholly precludes any legal access to content. We call on technology companies to work with governments to take the following steps, focused on reasonable, technically feasible solutions:

- Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and prosecution of offences and safeguarding the vulnerable;
- Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight; and
- Engage in consultation with governments and other stakeholders to facilitate legal access in a way that is substantive and genuinely influences design decisions.

IMPACT ON PUBLIC SAFETY

Law enforcement has a responsibility to protect citizens by investigating and prosecuting crime and safeguarding the vulnerable. Technology companies also have responsibilities and put in place terms of service for their users that provide them authority to act to protect the public. End-to-end encryption that precludes lawful access to the content of communications in any circumstances directly impacts these responsibilities, creating severe risks to public safety in two ways:

1. By severely undermining a company's own ability to identify and respond to violations of their terms of service. This includes responding to the most serious illegal content and activity on its platform, including child sexual exploitation and abuse, violent crime, terrorist propaganda and attack planning; and
2. By precluding the ability of law enforcement agencies to access content in limited circumstances where necessary and proportionate to investigate serious crimes and protect national security, where there is lawful authority to do so.

Concern about these risks has been brought into sharp focus by proposals to apply end-to-end encryption across major messaging services. UNICEF estimates that one in three internet users is a child. The WePROTECT Global Alliance – a coalition of 98 countries, 39 of the largest companies in the global technology industry, and 41 leading civil society organisations – set out clearly the severity of the risks posed to children online by inaccessible encrypted services in its 2019 Global Threat Assessment: "Publicly-accessible social media and communications platforms remain the most common methods for meeting and grooming children online. In 2018, Facebook Messenger was responsible for nearly 12 million of the 18.4 million worldwide reports of CSAM [child sexual abuse material to the US National Center for Missing and Exploited Children (NCMEC)]. These reports risk disappearing if end-to-end encryption is implemented by default, since current tools used to detect CSAM [child sexual

[1] https://documents-dds-ny un org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement

abuse material] do not work in end-to-end encrypted environments."[2] On 3 October 2019 NCMEC published a statement on this issue, stating that: "If end-to-end encryption is implemented without a solution in place to safeguard children, NCMEC estimates that more than half of its CyberTipline reports will vanish."[3] And on 11 December 2019, the United States and European Union (EU) issued a joint statement making clear that while encryption is important for protecting cyber security and privacy: "the use of warrant-proof encryption by terrorists and other criminals – including those who engage in online child sexual exploitation – compromises the ability of law enforcement agencies to protect victims and the public at large."[4]

RESPONSE

In light of these threats, there is increasing consensus across governments and international institutions that action must be taken: while encryption is vital and privacy and cyber security must be protected, that should not come at the expense of wholly precluding law enforcement, and the tech industry itself, from being able to act against the most serious illegal content and activity online.

In July 2019, the governments of the United Kingdom, United States, Australia, New Zealand and Canada issued a communique, concluding that: "tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can gain access to data in a readable and usable format. Those companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content."[5] On 8 October 2019, the Council of the EU adopted its conclusions on combating child sexual abuse, stating: "The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy and fair trial guarantees consistent with applicable law."[6]

The WePROTECT Global Alliance, NCMEC and a coalition of more than 100 child protection organisations and experts from around the world have all called for action to ensure that measures to increase privacy – including end-to-end encryption – should not come at the expense of children's safety[7].

CONCLUSION

We are committed to working with industry to develop reasonable proposals that will allow technology companies and governments to protect the public and their privacy, defend cyber security and human rights and support technological innovation. While this statement focuses on the challenges posed by end-to-end encryption, that commitment applies across the range of encrypted services available, including device encryption, custom encrypted applications and encryption across integrated platforms. We reiterate that data protection, respect for privacy and the importance of encryption as technology changes and global Internet standards are developed remain at the forefront of each state's legal framework. However, we challenge the assertion that public safety cannot be protected without compromising privacy or cyber security. We strongly believe that approaches protecting each of these important values are possible and strive to work with industry to collaborate on mutually agreeable solutions.

---

[2] WePROTECT Global Alliance, *2019 Global Threat Assessment*, available online at: <https //static1 squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf>,

[3] http://www missingkids.org/blog/2019/post-update/end-to-end-encryption

[4] https://www.consilium.europa eu/en/press/press-releases/2019/12/11/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/

[5] https://assets publishing service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_F NAL.pdf

[6] https://data.consilium.europa eu/doc/document/ST-12862-2019-INIT/en/pdf

[7] http://www2 paconsulting.com/rs/526-HZE-833/images/WePROTECT%202019%20Global%20Threat%20Assessment%20%28FINAL%29 pdf?_ga=2.109176709.1865852339.1591953966-1877278557.1591953966, http://www.missingkids.org/blog/2019/post-update/end-to-end-encryption, https://www.nspcc.org uk/globalassets/documents/policy/letter-to-mark-zuckerberg-february-2020.pdf

SIGNATORIES

Rt Hon Priti Patel MP, United Kingdom Secretary of State for the Home Department

William P. Barr, Attorney General of the United States

The Hon Peter Dutton MP, Australian Minister for Home Affairs

Hon Andrew Little MP, Minister of Justice, Minister Responsible for the GCSB, Minister Responsible for the NZSIS

The Honourable Bill Blair, Minister of Public Safety and Emergency Preparedness

India

Japan

11 October 2020