31 January 2018

Committee Secretary
Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

By email: le.committee@aph.gov.au

Dear Committee Secretary

The Digital Industry Group Incorporated (DIGI) welcomes the opportunity to make a submission to the Parliamentary Joint Standing Committee on Law Enforcement inquiry into *the impact of new and emerging information and communications technology (ICT).*

DIGI members include Facebook, Google, Microsoft, Oath and Twitter who collectively provide various digital services to Australians ranging from Internet search engines to digital communications platforms. These services and platforms facilitate new distribution, marketing and revenue generating channels for Australian businesses and content creators. They are also driving fundamental changes to the way that business is conducted, content is created and distributed, and helping people connect in meaningful ways with friends and family around interests or causes that matter to them.

DIGI thanks the Committee for the opportunity to make this submission. If you have any questions or require any additional information, please let me know.

Kind regards,

Nicole Buskiewicz
Managing Director
DIGI

Submission on the Impact of New and Emerging ICT on law enforcement

Overview

DIGI welcomes the Joint Committee's interest in exploring the impact of new and emerging information and communications technology (ICT) with particular reference to:

a. challenges facing Australian law enforcement agencies arising from new and emerging ICT;
b. the ICT capabilities of Australian law enforcement agencies;
c. engagement by Australian law enforcement agencies in our region;
d. the role and use of the dark web;
e. the role and use of encryption, encryption services and encrypted devices; and
f. other relevant matters.

As digital technologies have been become integrated into everyday life we are increasingly seeing all forms of human behaviour being replicated online and in digital environments. As a result, law enforcement investigations may now involve a digital element and / or interactions that have taken place over an electronic communications platform. This shift, as well as the challenges it has created for law enforcement, was recently acknowledged in a speech to the Australian Strategic Policy Institute (ASPI) by AFP Commissioner Andrew Colvin, who remarked: "The [criminal] environment is changing around us, and we're not adapting quickly enough."[1]

This submission will focus on parts A, B and E from the terms of reference above.

Challenges facing law enforcement agencies from new and emerging ICT

In DIGI member companies' experience, the biggest challenge facing law enforcement is education and training to understand that crimes committed online should be treated and investigated in the same way as physical crimes. Recently, Instagram (a DIGI member) was alerted to advice given by a police officer to a distressed mother whose daughter was being told to kill herself via Instagram. A police officer at her local station informed her that there was nothing that could be done despite the facts that (a) there are criminal laws prohibiting the use of carriage service to threaten, intimate or harass a person, (b) this type of conduct clearly violates Instagram's policies and will be promptly removed when Instagram becomes aware of it, and (c) Instagram has a well established process for responding to authorised law enforcement requests for data.

DIGI members conduct regular trainings and outreach with law enforcement agencies, but it is difficult to reach every single officer that might be presented with issues such as the one described above.

[1] Public Address by Commissioner Andrew Colvin, ASPI, 13 December 2017.

In the United Kingdom, law enforcement agencies have adopted a 'single point of contact' (SPOC) model. These designated SPOCs sit within each constabulary and are trained experts in how to obtain, interrogate and analyse digital information which can be instrumental in modern day investigations. The digital industry can focus their training efforts in a much more effective and targeted fashion, and officers within each constabulary have internal experts to draw on to ask questions, sanity check investigatory options and channel data access requests through.

This model came about through a recognition that it could be challenging to ensure that all law enforcement officers are equipped with the necessary knowledge and experience in requesting, interpreting and applying electronic data to an investigation. Recent advances in technologies such as encryption, cloud computing, connected devices, Big Data analytics, artificial intelligence, and virtual reality have presented law enforcement agencies with new methods and tactics for tackling crimes that involve an online element. Given the speed with which emerging technologies and platforms evolve, the SPOC model also makes it easier to keep officers up to date with the latest investigative tools and information.

In an interview in *The Australian* newspaper, Commissioner Colvin said that police have for too long been treating technology as the enemy rather than embracing it: "Let's treat the internet as an advantage for ourselves. We've been saying forever that crime is more complex, so why train my officers the way I was trained 28 years ago?"[2] DIGI agrees strongly with the Commissioner's statement, and believes the benefits afforded by technology cannot be overlooked when discussing modern day law enforcement. As an industry, we have developed a number of tools and taken a number of steps to assist Australian law enforcement in their efforts to fight crime, which we outline below.

ICT capabilities of Australian law enforcement agencies

As mentioned above, criminal activity that leverages technology has introduced new and unpredictable facets to modern investigations. These include promptly accessing and handling large amounts of data, being able to read/process unique sources of data in various file formats, and keeping their own information and devices secure.[3]

Law enforcement agencies are increasingly adopting a number of new and emerging technologies in response to these challenges. For example, when investigating a crime, incident details, situational information, and relevant documents can be accessed by officers in the field, who can collect evidence and upload it securely at the scene.[4] One real life example is the Domain Awareness System created by the New York Police Department and Microsoft, which is

[2] *Policing needs revolution to get ahead of criminals: AFP chief Andrew Colvin,* The Australian, 13 December 2017.
[3] Digital Transformation Enabling Next-Generation Public Safety and National Security, IDC Government Insights-Microsoft White Paper, May 2017.
[4] *Digital Transformation in Law Enforcement*: *13*, Microsoft Services, p. 7-8

one of the most sophisticated camera systems in the world that can show real-time footage from over 4,000 cameras and rapidly search video content to identify suspicious behaviour, for example, unattended bags. The system was so well received by visiting Victorian Premier Daniel Andrews that he announced he would investigate installing a similar system for Melbourne.[5]

Another example of how new and emerging technology is being used by law enforcement is in the area of virtual and mixed reality. An agent can record images of a crime scene on a 3D camera, and using a mixed reality headset, they can place virtual markers within the crime scene without disturbing the physical evidence. The information captured is combined into a 3D virtual model of the crime scene, which can later be used to reconstruct the crime scene virtually, allowing officers to revisit and explore the scene with mixed reality devices and applications.[6]

Mobile location data is another critical tool in any investigator's toolkit. The metadata relating to individuals who use electronic messaging platforms can be used to verify identity, triangulate location at any given time, and identify co-conspirators. All of this data is available to Australian law enforcement agencies through a legal request process.

There are a number of ways that various law enforcement agencies can lawfully request user data about suspected criminals held by companies. For the digital industry, this typically involves submitting a request through a company's dedicated process, which DIGI and members widely promote to law enforcement. Current data identifying the volume of requests being made to DIGI member companies are available through each company's transparency reports, which are easily accessible online. There are also processes in place for law enforcement to obtain access to data on an emergency basis where life is at imminent risk.

Access to the content of U.S. stored electronic communications is currently facilitated through the Mutual Legal Assistance Treaty (MLAT) process that Australia has entered into with the U.S. Government. This international standardised process allows a court or judge to ensure proportionality of each request is tested before data is accessed. However, our companies recognise that existing international standards for requesting data from other jurisdictions are outdated and in need of modernisation. Efforts are underway to develop new international agreements between like-minded governments which both respect the rights of the individual and provide for the legitimate interests of public safety agencies. The committee should examine the positive contribution these developments are making towards a more sustainable and lasting international framework that providers clarity and predictability for both requesting agencies and overseas companies.

Such information request processes are vitally important as they serve to protect the communications and transactions of the overwhelming majority of people who use digital

[5] *New York style Crime Surveillance Centre Planned for Melbourne*, The Age, 30 May 2016.
[6] *Ibid.*

services for good, in the regular course of their daily lives; while the internet and cloud computing has meant that their information can now be stored on remote servers rather than on-premise, this does not alter people's expectations around privacy. As an industry, we take the need to balance security and law enforcement agencies' need for information with the privacy rights of people who use our services, very seriously.

DIGI members provide guidelines for law enforcement agencies to assist them with making requests. In addition, DIGI coordinates training sessions with agencies like the AFP so they are familiar with members' respective law enforcement policies and processes to ensure requests are processed as expeditiously as possible. We also regularly engage with the Attorney-General's Department (now Home Affairs Department) to discuss emerging crime threats and respective efforts in the counter-terrorism and countering violent extremism space.

Finally, we have collaborated with peer companies to develop a set of principles – the Reform Government Surveillance Principles – and have engaged with legislatures around the world to encourage, inform, and guide them on the issues this debate raises.[7] We would encourage the committee to use these principles to guide its recommendations to government on future reform.

The role and use of encryption, encryption services and encrypted devices

Strong encryption is an essential foundation for cyber security, and the protection afforded by digital security and strong encryption is an important driver of consumer trust in the Internet.[8] UNESCO recognised in their 2016 report on Encryption and Human Rights that "the protection of encryption in relevant law and policy instruments from a human rights perspective is particularly important because encryption makes it possible to protect information and communication on the otherwise insecure communications platform that is the Internet."[9]

Encryption has become a fundamental part of our digitally connected world and economy. From keeping our banking data safe, safely storing our private photos and videos, or securely making payments online, encryption makes our digital social and economic lives function. Encryption is also a means to keeping government data secure, and how law enforcement agencies around the world have protected their information for decades.

US Senator Ron Wyden spoke at RightsCon last year highlighting that "encryption is one of the best defenses an individual has to protect himself or herself in the digital world," and noted that "....on balance government agencies' surveillance capabilities are at an all-time high."[10]

---

[7] Reform Government Surveillance Principles <https://www.reformgovernmentsurveillance.com/>.
[8] *How Strong Encryption Supports the Development of a Safe and Secure Internet: An Asia Pacific Perspective*, Analysis Mason 2016.
[9] Schulz, W., Van Hoboken, J., *Human Rights and Encryption*, UNESCO Publishing, 2016 <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>.
[10] Wyden, R (2016) "Wyden Calls for New Compact for Privacy and Security in the Digital Age" transcript, March 30, viewed 29 Jaunary 2018, <https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-new-compact-for-privacy-and-security-in-the-digital-age>.

There has been a great deal of speculation around the possible impacts of encryption on law enforcement investigations. It remains the case that the availability of much digital evidence is not affected by the use of encryption. Where encryption may limit the ability of a provider to disclose user content, metadata with considerable investigative value is available, and providers work closely with agencies to raise awareness of this and adapt processes and procedures for lawful access to such data accordingly.

Encryption is a mathematical tool, and like many aspects of computer science, it is evolving and changing. What was state-of-the-art 10 years ago is no longer considered appropriate to use in modern applications. Many of the fundamental building blocks of strong encryption (e.g., the Advanced Encryption Standard (AES)) are available to *anyone* as open-source code. Thus, efforts to impose limits on encryption by regulating how companies can deploy this ubiquitous technology will not necessarily achieve the goal of opening up a new trove of information that can be used for investigative purposes.

Great care must therefore be taken in developing future government policy around investigatory powers and avoid promulgating regulation that would compromise the effectiveness of encryption technology in the wider public and economic interest. A number of governments around the world have rejected such legal and market interventions in favour of a broader policy response which embraces international engagement, technical training for agencies, investment in new investigatory techniques and enhanced company engagement. We would urge the Committee to explore the benefits of this approach as part of its inquiry.