ASIC
Australian Securities & Investments Commission

Inquiry into the impact of new and emerging information and communications technology

Submission by the Australian Securities and Investments Commission

January 2018

Contents

A Overview

ASIC's submission

1 We welcome the opportunity to contribute to this inquiry into the impact of new and emerging information and communications technology. Our submission provides information on:

(a) some challenges facing ASIC arising from new and emerging information and communications technology (ICT), with a particular focus on the dark web and digitalisation;

(b) our ICT capabilities for meeting those challenges; and

(c) engagement with other law enforcement agencies on these issues.

2 We would be happy to provide further, more specific, information if the committee considers it would help the inquiry.

ASIC's role in law enforcement

3 ASIC's long-term vision for Australia's financial markets is that they operate in a fair, orderly and transparent manner so that national and international consumers, institutions and intermediaries have the trust and confidence to invest in our markets: see ASIC's Corporate Plan 2017–18 to 2020–21.

4 We are a primary law enforcement agency in relation to corporations, financial services and market misconduct. We regulate corporations, managed investment schemes, participants in the financial services industry and people engaged in credit activities under a number of Commonwealth laws. These laws include the *Corporations Act 2001* (Corporations Act), the *Australian Securities and Investments Commission Act 2001* (ASIC Act) and the *National Consumer Credit Protection Act 2009* (National Credit Act).

5 We use our enforcement powers in appropriate cases to detect and deal with unlawful conduct, to recover money and to prevent unlawful conduct before it happens. By doing this we deter future misconduct. We respond to breaches of laws within our regulatory responsibility, ranging from minor regulatory offences through to serious misconduct. Our credibility as an effective regulator, across all our areas of responsibility, depends in part on how well we use our enforcement powers: see Information Sheet 151 *ASIC's approach to enforcement* (INFO 151).

B Challenges for ASIC arising from new and emerging ICT

Key points

We are committed to supporting innovation and ensuring that the benefits of new technologies within the financial sector are shared with the market and consumers at large.

At the same time, developments in ICT can create risks for new forms of financial crime and pose a number of challenges to our ability to effectively detect, investigate and enforce the laws we administer. These challenges in particular include:

- the dark web and the use of virtual currencies on the dark web; and
- digitalisation of devices including encryption and cloud computing.

Dark web

6 The 'dark web' refers to the portion of the web that can only be accessed with additional networking protocols and software.

7 Within the dark web, marketplaces exist which enable criminals to:

(a) anonymously buy, sell and exchange malicious software; and

(b) access sensitive networks, payment card data, bank account information, brokerage account information and hacking services. Some of these activities occur within closed internet forums which require both sellers and purchasers to have demonstrated trust or reputation with forum administrators and users before being provided with access.

8 Traditionally the dark web was seen as a space that hosted marketplaces for drugs and/or narcotics. The US Department of Homeland Security estimated in 2015 that some of the more popular sites had 80,000 users. More recently in 2017, the US Justice Department shut down the dark marketplace Alpha Bay, a dark website, 10 times the size of Silk Road (an illegal marketplace shut down previously in 2013). Alpha Bay provided a marketplace for the sale of drugs as well as computer hacking tools. As the use of the dark web continues to grow, we are concerned that these marketplaces may be used to facilitate financial crime.

Surveillance of the dark web

9 The dark web presents a challenge for law enforcement as it is a space which is difficult to directly access. Hence, there is limited direct visibility for law enforcement agencies on conduct perpetuated through the dark web.

10 We face various challenges in building our surveillance capabilities to monitor the dark web. These include:

(a) the ability to assume identities in order to 'gain trust' to access closed dark web forums (and committing resources to maintaining 'trust');

(b) the protection of our systems and information (e.g. by being able to quarantine dark web access from our systems);

(c) the obscuring of internet protocol addresses (that help with the location of 'threat actors') through the use of 'TOR nodes';

Note: 'TOR nodes' refers to software that allows users to use the internet anonymously.

(d) the immediate jurisdictional access to 'threat actors' who are largely operating outside Australia; and

(e) lack of technological software and tools that have a specific focus on financial crimes, as typically the focus is on narcotics and terrorism.

11 The enforcement challenges posed by the dark web are compounded by the use of virtual currencies. Virtual currencies are non-tangible currencies that exist only in digital form (such as Bitcoin).

12 The main operational enforcement challenges presented by the use of virtual currency relate to the difficulty of tracing the currency to a particular identity due to:

(a) the use of virtual currency wallets which can easily be opened, transferred and concealed, usually without providing personally identifiable information;

(b) the use of 'mixing systems' or group signature algorithms to break links between payer wallets and payee wallets, or between a transaction and previous transactions;

Note: 'Mixing' systems involve taking coins from a number of users and outputting coins to different addresses that are not linked to the original users. 'Group signature algorithms' involve a payer providing a zero-knowledge proof that they own some coins from a list (without revealing which) while also leaking enough information to prevent double spending.

(c) obscuring IP addresses used to make a transaction or access a wallet; and

(d) transactions increasingly being conducted person-to-person and outside of exchanges.

Digitalisation

Encryption

13 The introduction of end-to-end encryption on digital devices and cloud computing has resulted in difficulties accessing and obtaining data and digital evidence.

14 Encryption is now widely used across message services, mobile devices and computers.

15 There has been a rapid increase in communication applications and devices that support end-to-end encrypted instant messaging. These communications are not stored on a centralised server owned by the service provider; instead, they can only be accessed from an end-point device (e.g. a mobile phone). The communications service provider is unable to access the content of communications that pass through the app. Some services also have a self-destruct function that, if set, will automatically delete messages from all sending and receiving devices after a certain amount of time elapses.

16 Similarly, data stored in the cloud may be encrypted, with some cloud service providers implementing a 'zero knowledge system' where all data held in the cloud is encrypted by the client before being transmitted and stored in the cloud. This means that even where data is able to be retrieved directly from the cloud, it cannot be decrypted without obtaining the encryption key from the client.

17 While encryption has clear benefits in safeguarding the privacy and security of sensitive data, it poses challenges for law enforcement agencies in obtaining access, in appropriate cases, to the encrypted content and devices.

18 These challenges are shared by law enforcement agencies globally. For example, in the United States, law enforcement agencies have referred to the problem of 'thousands of seized devices [sitting] in storage impervious to search warrants'. The Federal Bureau of Investigation (FBI) revealed that over an 11-month period it was unable to access over half of the devices in its possession, amounting to around 7,000 mobile devices. See note below.

> Note: The United States Department of Justice, 'Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy', 10 October 2017.

19 In response to this, for example, the United States Department of Justice has called for tech companies to implement 'responsible encryption' that allows law enforcement to access data: see note below. Responsible encryption is secure encryption that allows access only with judicial authorisation. Such encryption already exists (e.g. the central management of security keys and

operating system updates or a key recovery when a user forgets the password to decrypt a laptop).

> Note: The United States Department of Justice, 'Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy', 10 October 2017.

Cloud computing

20 Cloud computing is essentially the storing and potential processing of data offsite from a person's or entity's main premises. Often the data is stored overseas or replicated across numerous data centres.

21 In addition to the potential for data in the cloud to be encrypted, cloud computing creates some of the following challenges in terms of geographical disparity and forensic imaging:

(a) it can be difficult to identify the precise location of the data (which may be spread across multiple storage servers);

(b) if data is stored overseas, ASIC's immediate information-gathering powers no longer apply and the provider may be restricted by local laws as to the provision of any information to ASIC; and

(c) it can take a significant amount of time to capture data from a cloud storage location over the internet (depending on the server hosting the data and the internet connection used to acquire it), particularly for a large dataset.

Shift away from traditional telecommunications channels

22 There has been a shift away from the use of traditional telecommunications channels towards the use of communications and social media applications such as WhatsApp, Skype and Facebook for calls and instant messaging, as well as Voice over Internet Protocol (VOIP) calls.

23 This means that traditional sources of telecommunications information accessible to ASIC, such as call charge records, are becoming less and less useful.

24 We have limited capacity to compel the providers of these other communication channels to provide us with data, particularly where the provider is located overseas.

25 We are also unable to receive telecommunications intercept material (i.e. from a live stream of the content of communications carried over a telecommunications service), as we are not an 'interception agency' under the relevant legislation (see paragraph 34 below).

Growth in volume and complexity of data

26 The amount and complexity of data received by ASIC annually has been increasing substantially over recent years. This has created a number of challenges:

(a) There has been a rapid increase in mobile phone models and operating systems, and it can take up to 12 months for forensic analysis tools to support a new operating system or update.

(b) It can take a long time to forensically acquire and process the data.

(c) Significantly more storage capacity is required to house the data.

(d) It can be difficult to effectively and efficiently analyse the data to identify relevant evidentiary material. Traditional review methodologies reliant on keyword searches and manual review are becoming less practical.

C ASIC's response to the ICT challenges

Key points

This section gives an overview of the work undertaken by ASIC to respond to the ICT challenges. It discusses:

- ASIC's investment in data analytical tools to detect and respond to risks posed by new and emerging ICT; and
- law reforms which would support ASIC.

Continued investment in analytical and technological capabilities

27 We are committed to making ongoing investments in building our analytical and technological capabilities to ensure that we remain equipped to meet the risks posed by new and emerging ICT, including the challenges outlined earlier in this submission.

28 Some of our ongoing analytical and technological investments are outlined below:

(a) Tools and data analytics which provide visibility to activities in the dark web, including through the use of machine learning techniques and artificial intelligence.

(b) Enhanced analytics for social media monitoring, including programs which can be used to process large volumes of documents collected from various social media platforms such as Twitter and Facebook and produce targeted information.

(c) The use of analytics such as predictive coding to assist in the review of large volumes of data (technology assisted reviews (TAR)). TAR (and, in particular, predictive coding) uses machine learning and computer algorithms to assist investigators/reviewers in reviewing large data sets.

(d) Products to perform federated searches across intelligence data.

(e) Research into suitability of a big data environment to cater for large-volume, multi-format (pdf, images, videos, etc.) as well as multi-structured data. This is to alleviate challenges of dealing with evidence data stored on a range of mobile device and operating systems and the shift away from traditional telecommunication channels.

(f) Cloud-based solutions to deal with the growth in volume of data.

(g) An external data capture environment that will enable ASIC to receive a range of files from external stakeholders in a timely, secure, automated manner.

(h) A data science lab which will enable ASIC to experiment with a range of forensic tools in a controlled environment.

(i) Recruitment of data specialist expertise, as well as active engagement with external organisations specialising in data science research.

29 We have also had a focus on 'regtech' more generally (the use of technology for regulatory purposes) through our Innovation Hub. In appropriate cases this may include piloting the use of new technology in our regulatory work.

Law reform

30 We are supportive of law reforms that would:

(a) harmonise and enhance our search warrant powers with those in the Crimes Act (e.g. to allow ASIC to operate or secure electronic devices);

(b) provide ASIC with access to telecommunications intercept material to investigate and prosecute serious offences;

(c) allow ASIC to obtain and share telecommunications data with its foreign counterparts, which will help with, for example, the investigation of dark web activity facilitated by actors located overseas; and

(d) prescribe ASIC as a law enforcement agency in the Crimes Regulations 1990 for the purposes of Part 1AC of the Crimes Act.

ASIC Enforcement Review Taskforce

31 The ASIC Enforcement Review Taskforce released consultation papers in 2017 which included preliminary proposals for:

(a) ASIC Act search warrant powers to include ancillary powers that mirror the Crimes Act provisions. This would include powers to search, seize and copy electronic evidence to reflect modern business and communication practices in which information is stored and transmitted electronically rather than in paper form;

(b) ASIC to be able to receive telecommunications intercept material to investigate and prosecute serious offences.

32 The taskforce's final report is yet to be published.

IOSCO EMMoU

33 On 31 March 2017, the International Organisation of Securities Commissions (IOSCO) published the Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (PDF 1,014 KB) (EMMoU).

34 We are currently unable to become a full signatory to the EMMoU, and we have been seeking the legislative change necessary to do so. We must be able to demonstrate powers that allow us to obtain and share telecommunications data (i.e. telephone records and internet service provider records) with our foreign counterparts in order to help their conduct of criminal, civil and administrative matters.

D Ongoing engagement with other law enforcement agencies

Key points

This section gives an overview of the law enforcement agencies that we engage with domestically and internationally on ICT issues.

35 Many of the challenges we face in relation to new and emerging ICT are shared by other law enforcement agencies domestically and overseas.

36 We engage closely with other law enforcement agencies both directly and through participation in multi-agency forums and taskforces.

37 Domestically, the Commonwealth's core enforcement agencies working on financial crimes are ASIC, the AFP and the ATO, as well as ACIC and AUSTRAC. The Attorney-General's Department and the Department of Home Affairs are responsible for policy matters for criminal law and law enforcement, and for administering relevant laws including the Crimes Act and Criminal Code. The Commonwealth Director of Public Prosecutions is responsible for prosecuting alleged offences against Commonwealth law. We have also fostered strong relationships with state and territory police forces that face financial crime at a local level.

38 We are committed to building strong relationships with these agencies, and are supportive of a coordinated and strategic approach to combatting financial crime.

39 Internationally, we have developed strong formal and informal relationships with overseas regulators such as the Hong Kong Securities and Futures Commission, the Monetary Authority of Singapore, the United States Securities and Exchange Commission and the United Kingdom Financial Conduct Authority. We use these relationships to both share information and conduct joint investigations. We also engage with overseas regulators through IOSCO, including as a member of the IOSCO Asia-Pacific Regional Committee which addresses regional concerns.

Key terms

Term	Meaning in this document
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
Crimes Act	*Crimes Act 1914*
EMMoU	Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information
ICT	Information and communications technology
INFO 151 (for example)	An ASIC information sheet (in this example numbered 151)
IOSCO	International Organization of Securities Commissions
National Credit Act	*National Consumer Credit Protection Act 2009*
TAR	Technology assisted reviews
VOIP	Voice over Internet Protocol