Challenges and Opportunities of Prosecuting in the Digital Age

Hri Kumar Nair, *S.C.*
Deputy Attorney-General
Singapore

2nd Plenary Session: 12 September 2017

Introduction

1 We have a peculiar situation in Singapore. Our overall crime rate is low and we have a long established reputation as one of the world's safest cities. Crimes in the physical world are at an all-time low. Last year, we registered 30-year lows in violent crimes, housebreaking, theft and robbery.[1] But, the situation online is different. We saw exponential increases in online commercial crimes in 2014 and 2015 - by over 225% in 2014[2] and by almost 50% in 2015[3]. In 2016, we noticed a 65% increase in Internet love scams; over S$24 million was cheated from such scams in 2016 alone.[4]

2 In some ways, our rapid development is one of the causes. Singapore has one of the highest Internet penetration rates and *the* highest smartphone

[1] Singapore Police Force, Annual Crime Brief 2016 (https://www.police.gov.sg/~/media/spf/files/statistics/20170210_annual_crime_brief_2016.pdf).

[2] Singapore Police Force, Annual Crime Brief 2015 (https://www.police.gov.sg/~/media/spf/files/statistics/crimebrief2014.pdf).

[3] Singapore Police Force, Annual Crime Brief 2015 (https://www.police.gov.sg/~/media/spf/files/statistics/20160212_annual_crime_brief_2015.pdf).

[4] *Internet love scams up 65%, overall crime rate down 2.6% last year: Police*, The Straits Times, 10 February 2017 (http://www.straitstimes.com/singapore/internet-love-scams-up-65-overall-crime-rate-down-26-last-year-police)

penetration rate in the world. Nine out of ten persons in Singapore has a smartphone.[5] It is not an exaggeration to say that many Singaporeans live their lives on the Internet. They spend a sizeable chunk of their days on social media, communicating with one another or consuming news or entertainment. All this also takes place when they are supposed to be working!

3 Criminals are well aware of how ubiquitous smartphones and social media have become. Indeed and unfortunately, as is often the case, they are several steps ahead of most people in learning how to exploit the technology to relieve innocent people of their property. In fact, technology has given criminals the anonymity and security they have always craved.

4 The problems of prosecuting in the digital age are well-known. To name a few: (a) Criminals can hide their identities behind pseudonyms. (b) IP addresses can be easily masked. (c) Transactions can be multi-layered to make tracing difficult (d) Criminals can easily commit or direct their acts from the comfort of a different jurisdiction so that arrest, investigation and prosecution are difficult. (e) International fund transfers and, increasingly, virtual currencies, allow for cross-border movement of funds sometimes bypassing control mechanisms like anti-money laundering checks.

5 In this paper, I will highlight the challenges of investigating and prosecuting crimes in the digital age, but more importantly, how this also presents opportunities for prosecutors to be more effective. I will cite from actual cases that we have prosecuted in Singapore.

[5] http://www.todayonline.com/singapore/smartphone-penetration-singapore-highest-globally-survey

Crucial evidence can be found in plain sight by looking at the right places

6 The first major challenge of prosecuting in the digital age is that criminals can operate anonymously. Online identities can be created and discarded in an instant. Criminals can avoid interacting with the formal financial system, by either deceiving people into handing over details of existing bank accounts, or by using crypto-currencies. Traffic is often routed through many different IP addresses, making tracing the source of data very difficult. Often we find that our cases begin with nothing but a name, an email address, or a phone number, and very few promising leads to take the investigation further.

7 But criminals leave "footprints" from which we can trace their real identities. Crucial evidence can often be found in plain sight, simply by looking at the right places. Open Source Intelligence and Investigations ("OSINT") is an extremely valuable technique in our arsenal and we deploy it routinely to de-anonymise criminals.

8 In 2014, Singapore was hit by a spate of hackings. Government agencies, the national newspaper, commercial and religious organisations were targeted. The hacker called himself "The Messiah". He even released a video on YouTube threatening a massive cyber-attack on Singapore.

9 We had to find the person responsible and do so quickly. Given the seriousness of the threats made, our Prosecutors got involved at a very early stage.

10 The owners of one of the hacked websites had conducted their own OSINT searches online, and found an Internet forum where the hacker had

pseudonymously boasted about bringing down their site. The hacker's boasts included screenshots of him hacking into the website's server.

11 Using this information as a starting point, tech crime investigators from the Police, as well as our specialist tech crime prosecutors, then searched discussion forums used by hackers for other posts under the same pseudonym. Through this process, we were able to link various different pseudonyms used by the same hacker, based on contact information he provided and catch-phrases he used. We were able to find a live "tutorial" given by our hacker, where he provided a step-by-step demonstration on how to hack into Wi-Fi networks, complete with screenshots. From one of the screenshots, we saw all the Wi-Fi networks in the vicinity of the hacker. One of the Wi-Fi networks in the screenshot was named after a local clinic – the clinic itself was named after a road. From a simple Google search, we found out that the road that the clinic was named after, was in a residential neighbourhood in Kuala Lumpur, Malaysia.

12 Another smoking gun that we found through OSINT, was a Facebook post from one of the accounts we knew he was using. He wished a woman "Happy Birthday, Mum" on Facebook. The woman commented, "I should have never stood bail for you". We checked and found out that the woman's son had been charged for drug offences in Singapore, but had absconded and fled our jurisdiction. His cloak of anonymity had been lost – we knew who he was.

13 With help from Malaysia, the hacker was arrested in Kuala Lumpur and sent to Singapore. All this was accomplished in less than a fortnight. Eventually, we charged the hacker with over 160 charges. The evidence against him was

overwhelming. He pleaded guilty to 40 charges, of which 39 were under our Computer Misuse and Cybersecurity Act. He was sentenced to 4 years and 8 months in prison.

14 Other than de-anonymising individuals, open source investigation gives investigators the opportunity to observe many individuals simultaneously and draw conclusions on their relationships. Recently, a Greek ship captain was convicted of criminal breach of trust in Singapore, in relation to a large quantity of ship fuel that he was involved in misappropriating. After his appeal in Singapore's High Court was dismissed, he made an application to refer questions of law to our Court of Appeal. He was allowed to travel out of Singapore, pending the hearing of his case by the Court of Appeal. Even though the hearing was fixed quite soon thereafter, for many months, he kept delaying his return, claiming that he was very ill and receiving treatment in Athens. In the pre-digital age, we would have had to seek assistance from the Greek authorities if we needed to verify this. It might have taken some time. Through OSINT, we established who the ship captain's close friends and colleagues were within hours. Moreover, we saw a Facebook photo showing the captain at a birthday party. From the photos, we could tell that the party was on board a ship. The captain looked astonishingly well for someone who was very ill. The words on the birthday cake told us the name of the ship that he was on. Based on the date of the photo, and another quick open-source search, we could establish that, far from receiving treatment in Athens, the captain had been travelling on the high seas for months. We presented this information to our Courts to discredit the captain's excuses and obtained a warrant for his arrest.

15 The challenges I have cited therefore also present an opportunity. The lesson we learned from these cases is that the digital age has not altered fundamental human fallibilities – like the need to feel part of a community, even if it is a community of online criminals, or the need to gloat about one's achievements or even to be photographed having a good time. It is true that criminals will not use their real names on the Internet. The intelligent ones will even attempt to cover their digital tracks. But the perceived anonymity of the internet also makes some criminals careless or complacent. Technology allows prosecutors as well to penetrate walls which hitherto represented barriers to investigations. Creative thinking allows law enforcement and prosecutors to look for the interface between a criminal's online identity and the real world, and once that is found, criminals can quickly be identified, located and arrested.

With the right tools, relevant evidence can be found quickly and effectively

16 The second major challenge of the digital age is that prosecutors often have a vast amount of data and very little time to sieve out the crucial evidence. Sometimes, when electronic devices are seized, investigators tend to cautious and seize everything that may have relevant data. Sometimes, witnesses may hand over large volumes of data, expecting the investigator to go through everything to bring the offender to justice.

17 In our complex cases, there may be hundreds of gigabytes of data to go through. It is not humanly possible to go through everything. This must be a problem that many of you face in your own jurisdiction as well.

18 Not long ago, in a prosecution involving criminal breach of trust of millions of dollars from a church in Singapore, the investigators seized hundreds of

thousands of emails. We eventually identified 10,000 emails of interest. Out of these, over 1,000 emails were used at trial.

19 To deal with these cases effectively when they do arise, capabilities have to be developed in advance. To this end, we have implemented three strategies:

a. Firstly, the traditional model of prosecutors assessing the evidence after the investigation has concluded is not viable for complex cases. Prosecutors have to start working on complex investigations very early, be involved in the formulation of a case theory, and ensure that evidence is collected in a targeted and coordinated manner.

b. Secondly, automated document review tools are indispensable. We have been using one such tool for some years now. Our software can ingest huge repositories of data. It can sort the data based on file type – distinguishing between word documents, emails, pictures, videos, etc. It can also automatically draw out maps of communication between the various personalities that feature in the data and timelines of when the communications were exchanged. Most importantly, the software is also equipped with artificial intelligence; it can "learn" what data is relevant, by observing how the user identifies relevant and irrelevant items.

c. Thirdly, we are moving towards digitalising all our files. In the future, we anticipate that we will work solely based on digital copies of evidence, even if the original is seized in hardcopy. We are in the process of building a next generation digital workspace in our Chambers. We envision that this workspace will allow various prosecutors to concurrently work on a single case and for management to get updated and monitor progress in real time.

20 The digital age has forced us to develop and work with new tools, and presents a huge opportunity for prosecutors to do more with less. With the right tools, training and systems, prosecutors can develop the capability to oversee extremely complex investigations, with limited time and manpower.

A practical approach must be taken in relation to cloud evidence

21 The third major challenge of prosecuting in the digital age is presented by cloud computing. Large amounts of data are no longer stored on local computer hard disks, but in the "cloud". Traditional search and seizure processes to obtain evidence are irrelevant. Seizing and searching a computer in the possession of a suspect may not yield any useful evidence. To get such evidence, law enforcement would have to access data stored on remote servers.

22 Traditional mutual legal assistance frameworks are not the most appropriate means of getting cloud evidence. Cloud evidence is highly volatile. It can be altered or deleted before an MLA request even reaches the country where the servers are.

23 Investigators may need access to two kinds of information on the cloud: (a) Information that is publicly accessible by anyone. (b) Information that is only available to a specific account (e.g. an email or Facebook account) and can only be accessed by persons who have the login credentials to the account.

24 Most states will allow their investigators to access and download publicly-accessible information. As for information that can only be accessed with a username and password, one legally defensible way to get this information, is to do so *only* with consent. Consent could be obtained from the person whose account needs to be accessed, or from the cloud services provider.

25 If the evidence sought is incriminating, the suspect himself will never consent. The alternative might be to get the consent of the cloud service provider. Unfortunately, the provider also has a number of reasons to withhold consent. For example, fear of contractual liability to its users, or other potential legal liability from privacy or data protection laws of other jurisdictions. More simply, the provider may take the position that they are not bound to cooperate with law enforcement from another country, especially when there is no commercial incentive to do so.

26 An international consensus is necessary. Without such a consensus, there is a risk that investigators who access cloud evidence stored on servers located in another jurisdiction, may be exposing themselves to prosecution in another state, even though it was entirely permissible for them to do so under their domestic laws. We believe that an international framework must not limit investigators to only accessing cloud evidence with the consent of the data owner, whether that owner is the suspect or the service provider.

27 A sensible international framework will:

a. require countries to only allow access to cloud evidence if it is properly authorised by an appropriate law enforcement officer, in the same manner as is done for physical evidence within the country's physical jurisdiction; and

b. allow investigators to access data if they have *lawfully obtained the login credentials* to the account to which the data is available. This could include credentials obtained from another computer, or obtained by lawful order made to a person who has the credentials to disclose them.

28 The challenges presented by cloud evidence are common to all jurisdictions. We must develop new international norms that are sensible and account for the reality that the "cloud" knows no national boundaries. Only then can we prosecute effectively in the digital age.

Cybersecurity

29 I would like to end my remarks by saying that the best way to combat cybercrime is to prevent it in the first place. One aspect of preventing cybercrime is by enhancing cybersecurity. Through strong cybersecurity, criminals will know that computer systems are secured and that victims will report intrusions to the authorities. Thus, they are more likely to be deterred.

30 We hope that our draft Cybersecurity Bill, which is currently in the public consultation stage, will achieve this. In this Bill, we set out certain duties that will be imposed on owners of Critical Information Infrastructure ("CII"), i.e. computer systems that are necessary for the continuous delivery of essential services in Singapore.

31 If the Bill is passed, owners of CIIs will be required to: (i) provide information about the technical architecture of the CII system; (ii) report cybersecurity

incidents; (iii) conduct audits and risk assessments; and (iv) participate in any cybersecurity exercises that may be organised by the Government.

32 We think that effective investigations and prosecution, and sensible and carefully calibrated measures to secure our critical systems, will go a long way to protect Singapore and Singaporeans in the digital age.

33 Thank you.