CHALLENGES IN THE AGE OF CYBERSPACE

Paper delivered at the Fifth Annual Judicial Seminar on Commercial Litigation Hong Kong

Friday 21 October 2016

Robert McDougall*

Introduction

1 I have been asked to speak today on the topic of "challenges in the age of cyberspace". The particular area that I have chosen to speak about is cybercrime, with a specific emphasis on fraud. The development of the internet, coupled with ever more sophisticated and capable technology, has created unprecedented benefits and opportunities for private and commercial users. Unfortunately, those things have created equally profound benefits and opportunities for wrong-doers. A recognised commentator, Jonathon Clough states that the "internet is a paradise for those who prey upon the gullible, the greedy or the vulnerable" as "it provides unprecedented access to victims"[1].

2 Cybercrimes, such as fraud, can now be committed with relative ease, anonymity, and on a global scale. This presents significant challenges to users, businesses, lawmakers and enforcement agencies. The key challenges that I propose to discuss are: the scale of these crimes; the accessibility of the

*A Judge of the Supreme Court of New South Wales; Adjunct Professor, Faculty of Law, University of Technology, Sydney. The views expressed in this paper are my own, not necessarily those of my colleagues or of the Court. I acknowledge, with thanks, the contribution of my tipstaff for 2016, Lucy Jedlin BCom / Juris Doctor (Hons) in substantially preparing this paper. The virtues of this paper are hers; the defects are mine.

[1] Jonathon Clough, *Principles of Cybercrime* (2015, 2nd ed, Cambridge University Press) at 210

Internet; the anonymity facilitated by cyberspace; the portability of data; the ever-widening spread of the Internet; and the global reach of technology and the Internet, and in turn, cybercrime.

3 In this paper, after looking at those challenges, I will turn to legal issues such as jurisdiction and the criminal elements of cybercrimes. The global nature of these crimes reinforces the need for international action and inter-country cooperation both as to recognition of the criminal quality of "cybercrimes" and as to enforcement of laws aimed at suppressing them.

What is cyberspace / cybercrime?

4 The Internet was described by the United States Supreme Court in 1997 as a "network of connected computers … a unique medium – known to its users as cyberspace – located in no particular geographical location, but available to everyone, anywhere in the world"[2]. Cyberspace is essentially another term for "the Internet". The Internet was created in 1994, and has expanded globally and rapidly since its inception.

5 The evolution of the Internet created fresh opportunities for criminals, leading to the development of the term "cybercrime". It is difficult to define this term, or even to describe what it catches, in any comprehensive way – let alone, in a way that might have enduring significance. As technology constantly advances, criminals are developing new ways to commit crimes using the Internet. A limiting definition would do no more than create, not so much loopholes, as broad gateways for evasion.

6 There are a number of terms that may be used to describe cybercrime. The reach or denotation of that term must develop and evolve as technology does. Early in the age of the Internet, it was described as "computer crime". With the evolution of technology, it now encompasses "digital", "electronic" and "technology-enabled" crime, to name a few. It is important to note that the definition of cybercrime should not be constricting, as "the advancement of

[2] *Reno v American Civil Liberties Union* (1997) 521 US 844 at 849, 851

technology will almost certainly lead to a transformation of cybercrime which is why … some prefer to think of cybercrime as an ever-changing set of behaviours"[3].

7 In the light of this, in 2013, in a report on the National Plan to Combat Cybercrime, the Attorney-General stated[4]:

> In Australia, the term 'cybercrime' is used to describe both: crimes directed at computers or other information communications technologies (ICTs) (such as hacking and denial of service attacks), and crimes where computers or ICTs are an integral part of an offence (such as online fraud, identity theft and the distribution of child exploitation material).

8 The first of those categories is directed to offences that can only be committed in the digital world. The second category relates to "old crimes" that are being committed in new ways. This paper will focus on the second category of offences, and the challenges presented by advances in the technology which facilitates such crimes.

9 Society's increasing dependence on computer technology, and subsequently the Internet, created and developed what might be called the "market" for specific computer-related crimes.[5] Where there is a new technological advance, cyber criminals will find a way to exploit this. For example, the introduction of digital cameras was and continues to be exploited by child pornographers; and social media and electronic messaging sites are repeatedly used to stalk, harass and intimidate.[6]

10 One of the first major reported instances of cybercrime occurred in 2000, when a mass-mailed computer virus attacked approximately 45 million

[3] Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (2016, 1st ed, Routledge) at 13
[4] Attorney-General's Department, 'National Plan to Combat Cybercrime', (2013) at [4].This definition was taken from the *Protocol for Law Enforcement Agencies on Cybercrime Investigations* developed by the National Cybercrime Working Group
[5] Clough, above n 1 at 4
[6] Ibid

computers worldwide.[7] Cyber-attacks have increased in complexity, scale and anonymity since this event.

11 It was estimated that in 2015 the annual cost to the global economy of cyber-attacks was over US$400 billion.[8] That huge cost no doubt reflects the fact that modern cybercrimes, and cyber criminals, are "organised, financially motivated, technologically sophisticated and transnational".[9]

Overview of challenges

12 The rapid advance of modern technology exposes users to an ever-increasing array of risks. Fraudsters are no longer confined by borders or other physical constraints, as "the relatively clear borders and turf lines within the physical world are not replicated in the virtual realm"[10]. As Finklea states:

> High-speed Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals' abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims.[11]

13 In like vein, the Australian Securities and Investments Commission (ASIC) has noted that cyber-attacks have increased in "number, sophistication and complexity"[12]. This trend is expected to increase in the future, and presents a number of challenges for law enforcement officers, judicial officers, and users of the internet.

14 There are a number of key factors that make the Internet and technological advancements ideally suited to illegal activity, and a dangerous and

[7] KPMG International, 'Cyber Crime – A Growing Challenge for Governments', *Issues Monitor* (2011, vol 8) at [2]
[8] John Price, Australian Securities & Investments Commission, *Dealing with fraud: A regulator's perspective*, (Speech delivered at the Association of Certified Fraud Examiners Melbourne Chapter annual seminar, Melbourne, 10 November 2015)
[9] Clough, above n 1 at 3
[10] Kristin M Finklea, 'The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting US Law Enforcement', *Congressional Research Service* (2013) at 4
[11] Ibid at 5
[12] John Price, Australian Securities & Investments Commission, above n 8

challenging space for users and law enforcement officers. These include: scale, accessibility, anonymity, portability, technological advances, and global reach.

15 First, the scale of the Internet allows users to communicate with vast numbers of people worldwide, at any time of the day, in a simple and cost-efficient manner. This stands in stark contrast to pre-Internet methods of communication. The Internet creates an "unprecedented pool of potential offenders and victims" which in turn allows "offending to be committed on a scale that could not be achieved in the offline environment"[13]. A report prepared by KPMG in 2011 noted that "the international nature of cyber-crime results in the involvement of not only the target region, but also other countries or regions from where the attacks originate". This exemplifies the global nature of cybercrime, and demonstrates that the scale of its effects is potentially limitless.

16 Secondly, the ease with which people may access the Internet presents a significant challenge in cyberspace. It is accepted that the majority of households in the western world have access to the Internet. Clough asserts that in modern society "technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims"[14]. In 2012-13, over 80 per cent of adults in Australia, Canada and the United Kingdom had the ability to access the Internet, with an increase in the use of handheld devices and mobile phones.[15]

17 In recent times, there has been a shift from the use of computers, to tablets, mobile phones and other portable, smaller devices. Those devices have very similar functions and usability as computers. As a result, accessibility to the Internet has increased, and "frauds and schemes that were once conducted

[13] Clough, above n 1 at 6
[14] Ibid
[15] Ibid

face-to-face can now be carried out remotely from across the country or even across the world"[16].

18 It would be rare for individuals, at least in economically developed countries, to conduct their day-to-day business without the assistance of the Internet. There is an increasing expectation that services will be accessible through the Internet. For example, simple banking services, and government services such as Medicare and Centrelink, are making the move online. This has developed to the point that many service transactions can no longer be conducted face-to-face. As a result, those who access such services through the Internet are particularly vulnerable to fraud and other cybercrimes, as sensitive data is contained in these online portals.

19 The Internet "allows offenders to reach millions of potential victims at virtually no cost"[17]. The number of people using the Internet has increased over time, which in turn has led to an increase in the number of people conducting banking and other financial transactions online. Clough contends that the "increase in commercial and financial transactions conducted online provides an environment where people may be less wary of responding to emails or providing information via websites"[18]. This creates greater "opportunities for fraudsters to mimic legitimate organisations"[19]. In 2013, it was reported that 61% of adults engaged in banking online.[20] With the development of smartphone technology, it is likely that this figure has increased.

20 Thirdly, the anonymity that is created by the Internet acts as an incentive and advantage for those wishing to commit fraud or other illegal acts. Today, fraudsters have the ability to "deliberately conceal their identity online by the use of proxy servers, spoofed email or internet protocol (IP) addresses or anonymous emailers"[21]. Creating an online social media or email account does not require substantial identity verification. Offenders are able to create

[16] Finklea, above n 10 at 5
[17] Clough, above n 1 at 210
[18] Ibid at 211
[19] Ibid
[20] Ibid at 210
[21] Ibid at 6

realistic fake identities through those media. The global nature of technology means that online actions often pass through many jurisdictions, concealed at all levels by sophisticated techniques, making tracing of such crimes extremely difficult. The fraudster is able to commit crimes such as fraud and identity theft with relative anonymity, in a number of cases with the fraudster, like the wise and just testator of legal fiction, at home sitting in his (or her) armchair.

21 Fourthly, the portability and transferability of data have significantly facilitated the commission of cybercrimes. Over time, storage devices have become smaller while their storage capabilities have improved. Those committing illegal acts have the ability to store enormous amounts of data on small devices.[22] In addition, the storage capacity of mobile phones and tablet computers means that users are more vulnerable to attacks, as there is often a significant amount of valuable information held on such devices. Clough argues that "the portability and storage capacity of digital technology is such that loss or theft of a computer, smartphone, tablet or storage device may have disastrous consequences"[23]. Linked to the third point above, fraudsters are often able to access and transfer data held in such devices whilst remaining undetected by the owner of the device. This is particularly the case with "cloud" accounts.

22 Fifthly, and as Gillespie notes, "an undoubted challenge of cybercrime is the fact that technology advances so quickly"[24]. This presents challenges both for users of the Internet, and for regulators and those in the software security business, as the rapid advances in technology mean that those creating software to protect devices from hacking find it very difficult to keep up. ASIC noted that as technology develops, cyber threats become "increasingly diverse and sometimes unforeseeable".[25] In particular, as "the risk and sophistication of cyber-attacks [are] growing faster than traditional firewall

[22] Ibid
[23] Ibid at 219
[24] Gillespie, above n 3 at 10
[25] John Price, Australian Securities & Investments Commission, above n 8

antivirus technology can keep up"[26], users, financial services and businesses need to be commercially astute and implement strategies which "prevent, detect and respond to cyber risks"[27].

23 Finally, the global nature of the Internet presents a number of challenges. "[C]rimes committed via or with the aid of the Internet can quickly impact victims in multiple state and national jurisdictions"[28]. The virtual world allows criminals to operate without borders, providing them "with relative anonymity and a place to operate"[29]. To those who wish to use their computers or other devices to commit illegal activities, the only requirement is a working Internet connection. Notably, "as offenders may now communicate overseas as easily as next door, offenders may be present, and cause harm, anywhere there is an internet connection"[30]. This presents enormous difficulties for law enforcement, with issues such as jurisdiction and sovereign borders arising.

24 In May 2010, many Internet users fell victim to a "scareware" scam. The fraudsters caused users to believe that their computers had been infected with a particular virus, encouraging them to purchase new security software to eradicate it. Unsurprisingly, the security software was fake. This scam resulted in total losses of over US$100 million.[31] This case illustrates the scale of cybercrime, and the anonymity provided by the Internet. The perpetrators were not located, and these losses were not recovered.

25 That overview of some of the challenges that people may face in the age of cyberspace provides the background for a more detailed discussion of specific crimes that are being committed in cyberspace, such as fraud. To my mind, the biggest challenge faced by users and law enforcement officers alike is the rapid advance of the Internet. Technology is developing at an incredible

[26] Greg Medcraft, Australian Securities and Investments Commission, *Regulation for the future: Innovation, disruption and cyber resilience*, (Speech delivered at the AFR Banking & Wealth Summit 2016, Sydney, 6 April 2016)
[27] Ibid
[28] Finklea, above n 10 at 5
[29] Ibid at 5
[30] Clough, above n 1 at 7
[31] Finklea, above n 10 at 6; Federal Bureau of Investigation, "US Indicts Ohio Man and Two Foreign Residents in Alleged Ukraine-Based 'Scareware' Fraud Scheme that Caused $100 Million in Losses to Internet Victims Worldwide", press release, May 27, 2010

pace, with society constantly being pressured to acquire the latest technology. Cyber criminals are able to find new loopholes and new ways of exploiting such advances. It has been asserted that "humans are the weakest link"[32] in the cyber world. That is hardly surprising since, given the constant developments in technology, humans are simply unable to keep up with what they need to do to remain protected.

Fraud

26 Fraud of course has both a criminal and a civil aspect. In its criminal character, fraud is one of the most common types of cybercrime.

Types of fraud

27 There are a number of types of fraud which may be committed online, in the realm of cyberspace. These include[33]: fraudulent online sales; advance fee frauds; click frauds; electronic funds transfer (EFT) crime; fraudulent investments; identity crime; and phishing and hacking. Today, I intend to focus on advance fee frauds, EFT crimes, and phishing and hacking.

28 The most common example of an advance fee fraud is the 'Nigerian email scam', also known as the 'Nigerian 419' scam. The victim receives an email with the promise of a large payment of money if they will help the perpetrator transfer the money out of their country. The victim is asked to send their bank details so that their commission may be paid. In some cases, the victim is asked to pay a fee to help facilitate the transfer of the funds out of the country. Unsurprisingly, the funds never arrive, and the victim's money is taken. Recently, a prominent Nigerian email scammer, said to be responsible for global scams amassing more than US$60m, was arrested in Port Harcourt,

[32] Veda Advantage Information Services & Solutions Ltd, *Cybercrime and Fraud Report* (2015), available at: http://www.veda.com.au/sites/default/files/docs/ved464_fa_identity-fraud-report_hr.pdf, at 16

[33] Clough, above n 1 at 212-225

Nigeria. His techniques included "using malware to take over systems to compromise emails, as well as romance scams"[34].

29 Other forms of advance fee fraud include dating or romance scams, scams impersonating FBI or tax officials, or rental scams. Sometimes, the scammers will attempt to gain the trust of the victim, informing the victim of a series of unfortunate events in an attempt to win their sympathy. Despite the notoriety of such scams, a number of people still fall victim to them.

30 A recent crime that has occurred in the United States is known as 'cyber kidnapping'. In this case, the perpetrator persuades the victim, usually via phone, that he has kidnapped one of their loved ones and is holding them for ransom. The victim is then instructed to transfer money to accounts usually held offshore, and told that their loved one will be killed unless they obey. The perpetrator hacks into the victim's mobile phone, thereby being able to track the victim's every move. The victim, unaware that the perpetrator does not have the loved one, dutifully does as the perpetrator says.[35] It is difficult to trace such crimes and bring such perpetrators to justice.

31 EFT fraud is a common occurrence in Australia and worldwide. Technological developments have allowed fraudsters to commit these crimes with greater ease. Nowadays, "virtual cash may be moved in large volumes, between jurisdictions and with less chance of immediate detection"[36]. In Australia in 2001, a former government employee defrauded the Australian government of over $8 million, by transferring money from the Department of Finance and Administration to accounts in which he held an interest.[37] The prevalence of online banking, in particular mobile banking, allows people to be defrauded more easily, as there is often only an account number and a password or PIN in the way.

---

[34] BBC News, 'Online fraud: Top Nigerian Scammer arrested', 1 August 2016, available at: http://www.bbc.com/news/world-africa-36939751

[35] For a recent example of such fraud, see: http://www.smh.com.au/lifestyle/news-and-views/we-have-your-daughter-a-virtual-kidnapping-and-a-mothers-five-hours-of-hell-20161003-gru910.html

[36] Clough, above n 1 at 217

[37] *R v Muir* (unreported, ACT Supreme Court, 25 September 2001

32 Phishing can be defined as "the creation and use by criminals of e-mails and websites … in an attempt to gather personal, financial and sensitive information"[38]. These crimes commonly involve an email purporting to be from a bank stating that it needs certain information to verify the victim's account.

33 Hacking is a method of fraud that is particularly attractive to cyber criminals. As noted by Clough, "the ability for organisations to store large amounts of personal information, which is also easily searched and copied, provides an obvious target for unauthorised access"[39]. In 2013, the retailer Target was victim to a hacking incident, where the fraudsters gained access to approximately 40 million credit and debit card customer's records.[40]

Prevalence of fraud

34 One of the major problems with assessing the scale or prevalence of cyber fraud is that its reach is difficult to assess. There are several reasons for this. First, the definitions of cybercrime and fraud are constantly evolving, with no uniform definitions currently in operation. This means that precise statistics are difficult to calculate.

35 Secondly, there is evidence that suggests that some of these crimes are significantly under-reported. Gillespie cites a number of reasons for non-reporting including, that "it is a small amount of money, the victim may feel embarrassed, may wonder whether they themselves are complicit or do not know to whom they should address a complaint"[41].

36 Some crimes can go undetected because the fraudsters are using such sophisticated technology that the victim is unaware of the criminal activity. As Gillespie notes, there is a problem identifying victims of cybercrime where

[38] Binational Working Group on Cross-Border Mass Marketing Fraud, *Report on Phishing: A report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States* (2006), p. 4
[39] Clough, above n 1 at 224
[40] Ibid
[41] Gillespie, above n 3 at 143

people in fact do not know they have been victimised[42]. Anti-virus and other types of security protection also block a number of cyber-attacks. The security system may not report those unsuccessful attacks. Some users are subject to attacks "on almost a daily basis" but they are unaware "because they rely on automated protection systems"[43].

37 Another reason for the under-reporting of cyber-attacks is that many users see scam or phishing emails as a regular occurrence. The majority of people with an email address will at some stage receive an email that purports to be from their bank, or from a long-lost relative claiming they have received an inheritance. Gillespie poses the question of "how many [people] will have reported these emails as potentially fraudulent?"[44] In many cases, people will ignore them and see it as only a minor inconvenience, if there has been no damage suffered. It is usually only in the cases where the fraudsters are successful in their click-bait or other scheme, and where the victim has suffered a loss, that the fraud will be reported.

38 An additional reason for non-reporting is that the victim may feel embarrassed for "falling victim" to a scam, particularly where the scam is well-known, or where the amount is relatively small or the effect is non-monetary. However, even though the amount may be small for each victim, when these are multiplied infinitely, the effects are significant.

39 One of the largest banking security breaches in history occurred in the United States in 2014. The hackers infiltrated the servers of five United States banks, including JPMorgan Chase and others, stealing account information and other customer data. It remains unclear who the perpetrators of such attacks were, highlighting a further difficulty with prosecution of such crimes: the anonymity of the hackers. This case exemplifies the vulnerability of financial institutions, and the sophisticated methods used by hackers. Financial institutions need to continually update their fraud prevention software to stay responsive and defensive towards hackers' techniques.

[42] Ibid at 15
[43] Ibid
[44] Ibid at 143

40 Despite the apparent prevalence of these crimes, there have been relatively few convictions, in Australia or overseas. Some specific legislative responses, and the associated difficulties with prosecution and enforcement, will be discussed below.

Jurisdictional Issues in Cyberspace

41 One of the major problems with the prosecution of cybercrimes, such as fraud, is "jurisdiction". In the global realm of cyberspace, who has jurisdiction to deal with these crimes? A country's jurisdiction is often constrained by physical boundaries.[45] Its concern is to detect and prosecute crimes that occur within the area of its sovereignty. The key questions in cybercrimes are what is the relevant "event", and where does it occur. What is it that constitutes the essence of these crimes? Is it what is done? Or the effects of what is done? And where is the crime committed? Is it "the location where the conduct was initiated, the nationality of the offender, or the location where the effect was felt?"[46] Is it committed in two or all of those places?

42 Whilst criminals have the ability to operate across borders, law officers cannot,[47] at least absent both international cooperation and corresponding enabling domestic legislation. There are of course exceptions, where a country assumes a jurisdictional reach that may be considered to have "extra-territorial" effect. But even then, the assumption of extra-territorial jurisdiction is justified by the intra-territorial consequences of the criminal conduct.

43 What is meant by "jurisdiction" in this sense? Brenner provides one answer. She contends that the concept of jurisdiction encompasses three issues[48]:

(1) Jurisdiction to prescribe: a State's authority to make its own law applicable to activities, relations, or persons by enacting legislation, administrative rule, executive order or the determination of a court.

[45] Finklea, above n 10 at 10
[46] Kim Soukieh, *Cybercrime – The Shifting Doctrine of Jurisdiction,* (2011) 10 Can LR 221 at 226
[47] Finklea, above n 10 at 10
[48] Concepts taken from Susan Brenner & Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2003) 4(1) *Journal of High Technology Law*, 3

(2) Jurisdiction to adjudicate: a State's authority "to subject persons or entities to the process of its courts or administrative tribunals for the purpose of determining whether prescriptive law has been violated"[49].

(3) Jurisdiction to enforce: a State's authority to compel compliance or to penalise non-compliance with its laws or regulations.

44 It has been noted that whilst there is an array of problems with the regulation of cybercrime, jurisdictional issues have the potential to be "the most enduring obstacles to effective cybercrime policing globally"[50]. It is accepted that the primary difficulty with jurisdiction is enforcement. The global nature of cyberspace, and therefore cybercrime, presents significant problems in determining who has jurisdiction. As noted by Brenner:

> The interpretation of particularly the location of the act will create problems in cybercrime, where the origins and destinations of the crime are usually in different locations, and where the means, computer networks and IP packets, usually cross numerous territories.[51]

This in turn raises the question of identification of the activity that is proscribed, and the need to find some legitimate connection between that activity and the legitimate interests that the particular State's criminal laws seek to protect.

45 In most contract and tort claims, "territory" is the decisive factor in determining where jurisdiction lies. It is not so simple for cybercrimes. Soukieh asserts that whilst territoriality is often the decisive factor, the jurisdictional difficulty with cybercrimes arises from the fact that "the criminal conduct in cybercrimes may originate from a number of geographical locations, and its impact may have been global."[52] A further difficulty with cybercrimes, is that territoriality does not assist the determination of the location of the "proscribed event". The first step is to determine where the relevant "event" took place. Once that is done,

[49] Soukieh, above n 46 at 225
[50] Ibid at 234
[51] Brenner, above n 48 at 44
[52] Soukieh, above n 46 at 222

then territoriality may provide a proper basis for jurisdiction, depending on other intervening factors and the effects the particular crime has within other jurisdictions.

46 Few Australian cases have dealt with this jurisdictional issue in relation to cybercrimes. In *DPP v Sutcliffe*[53], the Victorian Supreme Court found that the applicable legislation had "extra-territorial" effect, and overturned the contrary decision of the Melbourne Magistrate's Court. The Melbourne Magistrate's Court had held that it lacked jurisdiction, because an essential element of the offence (stalking) had been committed outside Victoria. However, the Supreme Court found that as long as a 'substantial' part of the offence was committed within Victoria, the courts of that State had jurisdiction to deal with the matter.[54]

47 In another Australian case, the High Court held that where defamatory material was published on the internet, the relevant tort was committed where the material was downloaded from the server and read, not where it was uploaded.[55]

48 A recent United States case dealing with the issue of jurisdiction is that of Andrew Auernheimer. Auernheimer and his co-accused, Spitler, were accused of hacking into AT&T's website, gaining access to thousands of customers' email addresses. Auernheimer was charged with accessing a computer without authorisation. He was convicted and sentenced to three and a half years in prison. His conviction was quashed on appeal, with the Appeals Court finding that the trial court was not the proper "venue" for the case. The Appeals Court stated[56]:

> Here, none of the essential conduct elements of a violation of the New Jersey statute occurred in New Jersey. As discussed, neither Auernheimer nor Spitler accessed a computer in New Jersey. The disclosure did not occur

[53] (2001) VSC 243
[54] *DPP v Sutcliffe* (2001) VSC 243, at [45]
[55] *Gutnick v Dow Jones & Co Inc* [2002] HCA 56
[56] *United States of America v Andrew Auernheimer*, (United States Court of Appeals for the Third Circuit, April 11, 2014)

> there either. The sole disclosure of the data obtained was to the Gawker reporter. There was no allegation or evidence that the Gawker reporter was in New Jersey. Further, there was no evidence that any email addresses of any New Jersey residents were ever disclosed publicly in the Gawker article. The alleged violation of the New Jersey statute thus cannot confer venue for count one.

49 That case concerned only acts that occurred solely within the US. However, the Appeals Court focused on the concept of an "essential element", noting that the State could only prosecute where that element occurred within the State's territory. This case raises the important issue of determining where the proscribed act or activity occurred. The Appeals Court ultimately concluded that the essential element of the crime did not occur within New Jersey, despite the fact that the effects of the crime were felt there.

50 How, then, can the courts deal with jurisdictional issues? The most effective method of regulation and enforcement of these crimes is through cooperation between States, and a binding international agreement, acceded to and given legislative effect by participating States.

The Cybercrime Convention

51 The primary international document regulating cybercrime and cyber threats is the Council of Europe Convention on Cybercrime (the Cybercrime Convention)[57], created in 2001. The Cybercrime Convention is the first (and, so far, the only) international treaty to deal with cybercrime. The Convention came into force on 1 July 2004, and to date has 55 signatories. However, only 49 of the signatories have acceded to the treaty. (This is not a novel problem in international law.) Russia is not a signatory to the Convention. South Africa and Sweden are yet to ratify it. The United States acceded to the Convention in 2006, whilst Australia followed in 2012.

[57] Council of Europe, *Convention on Cybercrime* (ETS No. 185, Budapest, 23 November 2001)

52 The primary objective of the Cybercrime Convention "is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation"[58]. Whilst the Convention is plagued with enforcement issues, to date it is, as I have said, all that there is. The need for a comprehensive international legal treaty dealing with the issues and challenges in cyberspace is widely recognised, evident by the significant number of member and non-member states that have ratified or acceded to the Cybercrime Convention.

53 The relevant articles of the Cybercrime Convention, for present purposes, are Articles 7 and 8:

> **Article 7 – Computer-related forgery**
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A party may require an intent to defraud, or similar dishonest intention, before criminal liability attaches.
>
> **Article 8 – Computer-related fraud**
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
>
> (a) any input, alteration, deletion or suppression of computer data;
>
> (b) any interference with the functioning of a computer system,
>
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

[58] Council of Europe, *Convention on Cybercrime*, Details of Treaty No. 185, available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

54 The Cybercrime Convention attempts to clarify jurisdictional issues. Article 22(1)(a) confirms the territorial basis of jurisdiction, stating that "effect" and "citizenship" are bases for jurisdiction. However, where two parties are claiming jurisdiction, issues may still arise. In this instance, Article 22(5) states:

> When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the parties shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Australian legislation / regulation

55 Australia has acceded to the Cybercrime Convention, with the Convention coming into force in Australia on 1 March 2013, through amendments to the *Criminal Code Act 1995* (Cth). The Attorney General's Department noted that accession to the convention establishes a comprehensive, international framework and "also helps improve the ability of our agencies to work effectively with their overseas counterparts in responding to cybercrime"[59]. The Australian Government developed a National Plan to Combat Cybercrime[60], recognising that "the challenge presented by cybercrime is one that requires a coordinated national response"[61].

56 The explanatory memorandum to the amendments to the *Criminal Code Act* introduced in 2013 noted the growing threat posed by cybercrime to "Australian consumers, businesses and government"[62]. The memorandum applauded the work of the Convention, in introducing an international agreement to combat cybercrime. It stated[63]:

[59] Attorney-General's Department, *Cybercrime*, Available at: https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx
[60] Attorney-General's Department, above n 4
[61] Ibid at 6
[62] Parliament of Australia, Explanatory Memorandum to the Cybercrime Legislation Amendment Bill 2011, Outline
[63] Ibid

> The Convention is the first international treaty on crimes committed either against or via computer networks, dealing particularly with online fraud, offences related to child pornography and unauthorised access, use or modification of data stored on computers. The Convention's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

57 A key point in the development of new legislation must be to ensure that the legislative definitions are not limiting, so as to allow "criminals using new technologies to exploit loopholes"[64].

58 In Australia, fraud is defined as obtaining a monetary or other gain, or causing a loss, through deception. Under the *Criminal Code Act* these offences are found within Pt 7.3. In NSW, fraud is the subject of s 192E of the *Crimes Act 1900* (NSW). Online fraud has been recognised as a "complex area of the law" which is "capable of encompassing a wide range of forms of conduct"[65].

59 The amendments to the *Criminal Code Act* introduced Div 477 of Pt 10.7, giving effect to Articles 7 and 8 of the Cybercrime Convention. Part 10.7 deals with serious computer offences. It creates offences for unauthorised access, modification or impairment of data or electronic communications in a computer. Australia has intentionally not defined the term "computer" in its legislation. Clough notes that as technology evolves, "our conception of what is a 'computer' is constantly challenged"[66]. Mobile phones and tablets have similar capabilities and processing power to that of traditional "computers" so it is likely that they will fall under the definition. Interestingly, Clough also contends that the "increasing computerization of many household appliances and other everyday items presents a real danger of over-criminalisation"[67].

[64] Attorney-General's Department, above n 4 at 22
[65] Ian Lloyd, *Information Technology Law* (2014, 7th ed, Oxford University Press) at 223
[66] Clough, above n 1 at 59
[67] Ibid at 61

60 The United Kingdom has taken the same approach in its legislation.[68] The UK Law Commission noted the difficulties in defining such a term, arguing that any definition has the potential to be "under-inclusive" in the sense that it might not keep up with technological advancements, or "over-inclusive", as many household appliances now have remarkable technological capabilities.

61 The lack of a definition of "computer" may seem to create a potential issue for trial judges who are dealing with cases involving cybercrimes. The continuing advances of technology means that interpretation and application of this term will be constantly expanding and evolving. The Australian Committee that discussed the amendments to the *Criminal Code Act* in 2001[69] recognised that problems of over-criminalisation would be unlikely to be addressed satisfactorily through limiting the definition of the term "computer". It concluded that those problems are better managed through an assessment of the scope of the offence.[70] The best place for this is in the Courts, on the basis that such terms can be given their "ordinary meaning". That ordinary meaning can be adapted to the particular circumstances of the case,[71] so as to accommodate advances and developments in technology.

62 Although in a very different context, and dealing with different technologies, the issue of whether legislation should be construed so as to accommodate changing technologies was discussed in *Wilson v Commissioner of Stamp Duties*[72]. In that case, Kirby P stated:

> These are times of particularly rapid technological change. The legislature, with the many pressures upon it, may have insufficient time quickly to elaborate statutory provisions specifically to refer to new technological developments. Accordingly, it may be an appropriate modern canon of statutory construction to adapt language of generality, although originally

[68] *Computer Misuse Act 1990* (UK); Law Commission (UK), *Computer misuse* (1989), [3.39]
[69] Model Criminal Code Officers Committee, *Computer offences* (2001)
[70] Clough, above n 1 at 61-62
[71] Ibid at 62
[72] (1988) 13 NSWLR 77

designed to apply to an earlier technology, to apply to the supervening technology as well.[73]

63 In relation to the jurisdictional issue, s 15.1 of the *Criminal Code Act* extends the geographical reach of the Act. Section 15.1(1)(b) states that the Act applies if the conduct constituting the alleged offence occurs wholly outside Australia so long as the result of that conduct occurs wholly or partly in Australia, or the offender is an Australian citizen[74]. This appears to clarify the jurisdictional issues apparent from cases such as *DPP v Sutcliffe*.

64 A recent news article in Australia suggested that the focus of an upcoming review into Australia's intelligence agencies would be on cybercrime. Cyberspace, and developments in technology, pose a serious threat to not only financial institutions but to governments. Dr Tobias Feakin states "post Snowden … there needs to be a review in understanding how our agencies reshape themselves towards the goal of being able to carry out signals intelligence"[75]. Over the past few years in particular, governments have been spending more and more money on technology, in an attempt to protect themselves from such attacks. One of the biggest issues plaguing governments comes from terrorist organisations, who utilise cyberspace to plan attacks, as well as to recruit new followers. Whilst outside the scope of this paper, the use of cyberspace in facilitating terrorist attacks is a real challenge for governments and law enforcement officers.

65 One of the common problems found in international law is that of enforcement. It is accepted that international courts "have very limited powers"[76], making enforcement difficult. Enforcement must rely on domestic legislation. However, the principle of state sovereignty means that countries

[73] *Wilson v Commissioner of Stamp Duties* (1988) 13 NSWLR 77 at 78
[74] Criminal Code Act 1995 (Cth), s 15(1)(c)
[75] ABC News, 'Cyber attack threats to be focus of Australia's intelligence agencies review', 19 September 2016, available at: http://www.abc.net.au/news/2016-09-19/australia's-intelligence-agencies-to-be-reviewed/7857906
[76] Krishna Prasad, 'Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework', *Australian Counter Terrorism Conference* (2012) at 10

can legislate on a matter in a way they see fit, as such, the "legal procedures and systems vary" considerably from country to country[77].

66 Until States recognise the value of international law, its enforcement will be limited. Soukieh states[78]:

> Jurisdictional issues will continue to frustrate cybercrime investigations and prosecutions at every level, until all core stakeholders begin to see international treaties, not as devaluing of sovereignty, but as a pre-requisite to international trade and security.

67 As I have noted, a major difficulty with prosecution and enforcement of cybercrime is that the acts constituting the offence can take part in many different places over the world. In some cases, there may be several perpetrators who are located in different continents, working together. With the aid of the Internet, they are able to communicate seamlessly. In such a case, it is advantageous for the prosecuting country to charge the two offenders together – but the question remains, which country has jurisdiction?

68 A recent high-profile international case is that of Sergei Tsurikov. Tsurikov was convicted by the United States District Court in Georgia in 2014 for conspiracy to commit fraud, resulting in the loss of over US$9.4 million.[79] The crimes related to the hacking of a US credit card processor. Using sophisticated hacking techniques, the offenders (Tsurikov and his co-defendants) were able to compromise the data encryption and security methods used by RBS Bank, accessing the accounts of "payroll debit cards", and raising the limits on such cards. The offenders then provided "cashers" with counterfeit payroll debit cards that were then used in over 2100 ATMs all over the world to withdraw over US$9 million.[80] The cashers kept a percentage of their funds withdrawn, and transferred the rest back to Tsurikov and his co-defendants.

---

[77] Ibid
[78] Soukeih, above n 46 at 223
[79] Clough, above n 1 at 3; US Department of Justice, 'International hacker sentenced', Press Release (24 October 2014) https://www.justice.gov/usao-ndga/pr/international-hacker-sentenced
[80] US Department of Justice, 'International hacker sentenced', Press Release (24 October 2014)

69 Tsurikov, who had pleaded guilty to these offences, was sentenced to eleven years in a United States prison, and ordered to pay US$8,400,000 in restitution. The significance of his crime lies in the fact that "it was organised, financially motivated, technologically sophisticated and transnational"[81]. The hackers were able to watch in real-time the withdrawal from ATMs all over the world through their access to RBS' online system. This exemplifies the ability of technology to assist fraudsters in their methods. In this case, the US Department of Justice noted the assistance provided by other countries in the prosecution of Tsurikov and his co-defendants, reaffirming the importance of international cooperation.

The issue of dual criminality

70 In relation to extra-territorial crimes, one of the hurdles that countries must face in attempting to prosecute perpetrators of cybercrimes, is the issue of dual criminality. If a country wishes to extradite a perpetrator to face prosecution in its courts, the country where the perpetrator is found must recognise the alleged offence, meaning that it must be an offence in both countries, usually with a minimum jail term of 12 months.[82]

71 In the infamous case of the 'Love Bug' virus, the alleged perpetrator was a student in the Philippines. The US wished to prosecute the perpetrator, as he attempted to hack into banks in the US through the distribution of an e-mail virus. At that time, the Philippines did not have laws under which the perpetrator could be charged. Thus, he could not be extradited to the US. Soukeih notes that the requirement for double criminality exemplifies "the tension between one country's desire to enforce its laws and another country's determination to preserve its legal sovereignty"[83].

[81] Clough, above n 1 at 3
[82] Soukeih, above n 46 at 230
[83] Ibid

72 An interesting case demonstrating the need for international cooperation to enforce convictions of these crimes is *United States v Gorshkov*[84]. Gorshkov, a Russian national was sentenced to 36 months in prison in the US for crimes of conspiracy, computer crimes, and fraud. Russia had no extradition treaty with the US. Gorshkov was enticed to the US by undercover agents posing as potential employers, and arrested on arrival. Russia was uncooperative in the investigation, so the US agents hacked into computers in Russia to find information on Gorshkov. Russia then took the drastic step of charging those agents with unauthorised access. This case exemplifies the need for international cooperation in order to effectively combat cybercrimes and cyber threats. To this end, Soukieh asserts[85]:

> Cybercrime policing, in particular, is only as effective as its weakest link, and while nations refrain from participating in treaty making and collective law enforcement, the prosecution of offenders, hiding behind so-called safe-harbour provisions, will continue to prove difficult.

73 It is well-accepted that international courts have very limited enforcement mechanisms and powers. A paper by Prasad, whilst focusing on cyber terrorism specifically as opposed to cybercrimes more generally, noted[86]:

> The rapid advancement of computer technology has increased the frequency and impact of cyberterrorism worldwide. These cyberterorrists continue to operate in a borderless environment with the knowledge that there is no single international legislation. Governments have varying technical competence to deal with cyber … acts and the coordination among law enforcement authorities are restricted by foreign policies and ideologies.

74 Prasad notes that "the current international legislative environment provides very limited or no deterrence for perpetrators committing"[87] cybercrimes. She asserts that "coordinated international action is the only way to tackle this

[84] *United States v Gorshkov* (Case No: CRo00-550C, US District Court for the Western District Court of Washington, 2001)
[85] Soukieh, above n 46 at 235
[86] Prasad, above n 75 at 14
[87] Ibid

global issue"[88], which can be achieved through the implementation of national legislation, consistent with international guidelines.

75 One of the primary reasons cited for states not wanting to cooperate on this issue is their desire to protect their sovereignty, creating resistance to international bodies instructing them how to legislate in particular areas. States "are understandably protective of their right to impose their own standards … particularly when we consider the myriad interests that come into play when seeking to regulate the internet and other new technologies."[89] Without international cooperation, jurisdiction and enforcement issues remain alive, stymieing prosecutions and deterrence of cybercrimes. Deterrence requires detection of the crime, identification and prosecution of the offender, and (upon conviction) appropriate punishment.

76 The "Botnet virus" is essentially a program that logs users' keystrokes and records this data and forwards it to cyber criminals. They are able to decipher users' online banking information and other useful data. This data can then be used to steal personal and financial information. In one particular case, highlighting the difficulties faced by law enforcement in relation to the anonymity provided by the Internet, the United States filed complaints against 13 "John Doe" defendants who were believed to be the perpetrators of Botnet virus crimes. The US faced extreme difficulties in identifying the alleged perpetrators, and it was thought that many were foreign nationals residing in different jurisdictions. The global nature of the Internet and the anonymity provided by the Internet meant they were never brought to justice.

Conclusion

77 I have sought to highlight some of the problems faced by modern society flowing from the misuse of computer technology and cyberspace. Cyber criminals "rely on constantly advancing technology and near anonymity in

[88] Ibid
[89] Clough, above n 1 at 24

cyberspace to work both within and across borders and jurisdictions"[90]. This creates significant problems for users of technology, and those trying to prevent cyber-attacks from occurring. The anonymity generated by the Internet makes law enforcement extremely difficult. The rapid evolution of the Internet allows criminals to operate in a borderless virtual world, utilising their anonymity or different identities to remain undetected. Businesses and users must remain up-to-date with technological developments in an attempt to protect themselves from this ever-growing threat. And unless nations take effective and cooperative steps to combat cybercrime, the battle will be lost.

[90] Finklea, above n 10 at 8