SUBMISSION Combatting Crime as a Service

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

FROM: Professor Rick Sarre
[redacted]

12 October 2025

Introduction

I write as an academic (of some 35 years) in the fields of law, criminology, policing and private security. I also make this submission with the endorsement of the Australian Crime Prevention Council, through its National Chairman His Honour Judge Rauf Soulio, and ACPC South Australian Executive Member His Honour Auxiliary Judge Peter Norman.

In summary, my submission directs the Committee's attention to a recent (2023) academic research book that examines the nature and impact of technology-driven cybercrime methodologies, and the tools needed to combat the scourge of cybercrime. I include a short summary of the chapters of all contributors, and then a full chapter of mine from that book. My chapter discusses the willingness and aptitude of those who share this new-found connected cyberspace to engage in criminality. It then sets out a range of policy options to confront this dilemma if private sector operatives and government security agencies and police engage in dialogue to pursue joint strategic operations.

The Submission

A book was published in 2023 entitled *Cybercrime in the Pandemic Digital Age and Beyond,* (Palgrave Macmillan), edited by Professor Russell G Smith, Flinders University, Emeritus Professor Rick Sarre, University of South Australia, Dr Lennon Chang, Monash University, Victoria, and Dr Laurie Lau, Asia Pacific Association of Technology and Society, Hong Kong.

The book contains a great deal of information regarding the nature and impact of technology-driven cybercrime methodologies. It was framed as a post-pandemic reflection, but its observations are valuable today as a blueprint for the future. The book sets out the challenges and opportunities for law enforcement in Australia regarding technology-driven crime generally. It suggests a preferred regulatory framework.

Table of Contents

Chapter 3 – Pandemics and fraud: Learning from the coronavirus pandemic and its antecedents, Michael Levi

Chapter 4 – The human element of online consumer scams arising from the coronavirus pandemic, Monica T. Whitty

Chapter 5 – State-sponsored economic espionage in cyberspace: Risks and preparedness during and after the pandemic, Hedi Nasheri

Chapter 6 – Virtual kidnapping: Online scams with 'Asian characteristics' during the pandemic, Lennon Yao-Chung Chang, You Zhou and Duc Phan Huy

Chapter 7 – Lessons in a time of pestilence. The relevance of international cybercrime conventions to controlling post-pandemic cybercrime, Jonathan Clough

Chapter 8 – Domestic laws governing post-pandemic crime and criminal justice, Gregor Urbas and Marcus Smith

Chapter 9 – Perspectives on policing post-pandemic cybercrime, Rick Sarre

Chapter 10 – Digital criminal courts: The place or space of (post-)pandemic justice, Carolyn McKay and Kristin Macintosh

Chapter 11 – Online messaging as a cybercrime prevention tool in the post-pandemic age, Richard Wortley and Jeremy Prichard

Chapter 12 – Artificial intelligence, COVID-19, and crime: Charting the origins and expansion of dystopian and utopian narratives, Sanja Milivojevic

Chapter 13 – Conclusions: Minimizing crime risks in pandemics of the future, Rick Sarre

Jill Slay examined the use of illegal manipulation of digital technologies during and following the current pandemic, offering us an opportunity to view some of the societal changes and disruptions which occurred. She drew our attention to emerging technologies such as the Internet of Things (or IoT, namely physical objects with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks). She highlighted the power of quantum computing and the broad usage of satellite services for communications and earth observation. She described how modelling using the Cyber Kill Chain provides a method whereby the technical context of transactions can be envisaged within a bank, a satellite, or any other institution during, before or after a pandemic.

Michael Levi discussed the patterns of and responses to a range of economic crimes, offline and online, short-term and longer-term. He wrote of the importance of measuring cyberfraud victimisation, using both official recorded data and victimisation surveys. He maintained that they are essential tools in considering the scale of some components of these problems in what he termed 'human security'.

Monica Whitty wrote of the way in which there was a tectonic plate shift of the workforce during the pandemic from the office to work-from-home, and, for some, consequential and enduring high levels of stress and anxiety. During this time, the number of victims and financial losses from cybercrime increased dramatically. She introduced readers to various psychological theories to understand human vulnerabilities to cyber scams (e.g., romance scams, investment scams, phishing, consumer scams). Importantly, she provided an insight into how we are to develop resilience to these scams post-pandemic. She critiqued the criminological theories to explain the conditions that may lead to an increased chance that fraud will occur.

Hedi Nasheri shifted our attention to the way in which both public and private sectors must be able to act and respond to threats with preparedness. She wrote of the ongoing threats, especially to the United States, of what is suspected to be state-sponsored espionage. There is little doubt in the global realm that cyber sleuthing and stalking often emanates from China, but it is not confined to the East. Western democracies are not blameless in this regard. One need only think of Australia's involvement in the interceptions that preceded the East Timor and Australian Maritime Boundary Treaty and the rights appertaining thereto to gain an appreciation of the global reach of state-sponsored cyber stalking.

Lennon Chang focused our attention on the scams that target people with a specific cultural and social background, an example of which is virtual kidnapping of international students. Although such 'kidnapping' is not a new phenomenon, lockdowns and travel bans created additional opportunities for it, especially with Chinese students. He reminded us that the Australian Securities and Investments Commission issued a broadly-based warning in May 2021 that scammers are using the COVID-19 pandemic to target Australian small businesses with a range of scams including phishing, vaccine supply scams and email ransomware. Moreover, he noted, online bullying and hate speech are becoming more invasive.

Jonathan Clough reminded us that much of the most effective work of cybercrime investigation and prosecution continues at the local, regional and bilateral levels. But the most effective prophylactic responses will emerge only when international cooperation can be harnessed and coalesced. The Budapest Convention, which, as Clough asserts, "has the potential to bring together disparate voices, establish areas of common agreement and remove the sense of exclusion" is but a start. The world, Professor Clough reminds us, will need to remain on the alert for the next pandemic wave, and the next iteration of criminality to follow.

Gregor Urbas and Marcus Smith highlighted the way criminal justice systems have had to deal with specific offences enacted in response to public health concerns. Restrictions on personal movement and international travel, and prevention measures such as mandated mask-wearing, were enforced through fines and imprisonment for people who, they might have thought, were exercising their rights as law-abiding (sovereign) citizens to remain aloof from governmental strictures. The conduct of legal proceedings has also been affected, said the authors, with an increased use of remote hearings, technological forms of document submission, and judge alone hearings. Bail, trial and sentencing procedures were all modified, and these changes are likely to continue well beyond the pandemic.

Rick Sarre addressed the way we need to monitor and police the new cybercrime landscape. He reviewed the role the private sector can play. He wrote of the important role of the private sector but added that governments cannot adopt a 'hands-off' approach and allow the private sector free rein in their quest to defeat cybercrime. Rather, he asserted, it is imperative that governments regulate and monitor the interventions by the private sector into citizens' daily lives, even if it is done in the name of cyber security, lest these interventions leave people more vulnerable to policy over-reach and breaches of privacy.

Carolyn McKay and Kristin Macintosh directed our attention to the effect of the pandemic on the criminal courts. We witnessed, they wrote, suspension of jury trials, adjourned hearings and 'pivoting' of systems to remote procedures. Integral to this sudden change was an array of digital communication technologies: audio and audio-visual links as well as third party proprietary platforms. They concluded that the era of digital criminal justice has begun. However, within this new age of spatially dispersed criminal justice, and even with a recognition of virtuality as part of post-pandemic reality, there remains an indispensable role

for face-to-face, high level decision-making processes to be undertaken in shared physical places. In other words, the logics of online versus face-to-face interactions remain distinct.

Richard Wortley and Jeremy Prichard made the case for the use of online warning messages as a key cybercrime prevention tool. They argued that the extent of the cybercrime problem cannot be tackled through traditional law enforcement tactics alone; we must explore prevention approaches aimed at reducing the incidence of cybercrime in the first place. Internet warning messages are one technique that will help make the Internet a safer environment for users. Automated cybercrime prevention messages can mimic key aspects of criminal business models. They, too, can be rolled out quickly and economically on a large scale. They are worth considering, said the authors, even if they only deter, deflect, or disrupt a fraction of cybercrime.

Sanja Milivojevic highlighted the role played by artificial intelligence in the pandemic world. She noted that we rely on technology and science as essential tools that can 'tame' the 'beast.' On the other hand, technological innovations can be deemed hazardous, if not fatal, for individuals and communities. There is no doubt, she said, that in the future of digital frontier technologies such as the Internet of algorithms, artificial intelligence, interconnected smart devices and autonomous machines there will be unwanted outcomes. She declared that the "risky" times of the global pandemic were linked to criminal activity in traditional and social media and the policy development in the Global North. She concluded that many interventions designed to disrupt cybercrime led to further restrictions of fundamental human rights and civil liberties rather than crime prevention, inserting a tricky conundrum into the plans of cybersecurity policymakers.

My contribution to the book

Copyright restrictions prohibit me from sending pdfs of the entire book, or pdfs of my contributions, but I can include one relevant chapter of my own in Word form, which I do now.

Chapter 9 - Perspectives on policing post pandemic cybercrime

Rick Sarre

Introduction

The massive changes in societal expectations of human and business connectivity and the shifts in technology that have been designed to meet these demands are profound. The modern world is well-entrenched in the digital age. It is dependent upon its complex features and storage capabilities that can accommodate the flood of data from millions of sensors in our commercial hubs, the streams of visual images generated by users of social networks and the information produced by those who use mobile devices. This was foreshadowed in the past.

> The new economy is more about analysing rapid real-time flows of unstructured data … The world will bristle with connected sensors so that people will leave a digital trail wherever they go … (Economist 2017, p. 24)

Indeed, the digital world expands exponentially year by year, and the pandemic has only served to hasten this growth as more people move their social lives online and more and more workers are asked to log in to their workplaces remotely from home. Even before the pandemic began, a market research firm predicted in 2017 that the digital universe (the amount of data created and copied) would reach 180 zettabytes (180 followed by 21 zeros) by 2025 (Economist 2017). This level of global connectivity has led to a massive expansion of

instantaneous commercial expediency, enhanced trade opportunities and heightened levels of personal networking.

However, there is a significant downside to this revolution: the willingness and aptitude of those who share this new-found connected cyberspace to engage in criminality. Estimates a decade ago reported that cybercrime was costing the global economy billions of dollars annually (Broadhurst and Chang 2013; Sarre, Brooks, Smith and Draper 2014; Australian Crime Commission 2015), and losses continue to expand virtually unabated. A most recent estimate by the Australian Competition and Consumer Commission (ACCC), based on its analysis of more than 560,000 reports of losses in 2021, calculated the annual costs of consumer cybercrime in Australia alone to be above $A2 billion (ACCC 2022). Investment scams were the highest loss category (A$701 million), followed by payment redirection scams (A$227 million) and romance scams (A$142 million). However, as approximately one-third of victims do not report scams, the ACCC estimated actual losses far exceeded this amount. It is no exaggeration to say that 'malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity' (Australian Cyber Security Centre 2017, p. 16). There is little doubt that the pandemic from 2020 to the present day has only served to heighten these risks and losses.

The phenomenon of cybercrime

There are variable definitions of cybercrime. It has been variously referred to as 'computer crime', 'computer-related crime', 'hi-tech crime', 'technology-enabled crime', 'e-crime', or 'cyberspace crime' (Chang 2012). Grabosky (2007) helpfully classified three general forms, including crimes where the computer is used as the instrument of crime, crimes where the computer is incidental to the offence, and crimes where the computer is the target of crime. McGuire and Dowling (2013) developed the now accepted concept of classifying cybercrime as 'cyber-enabled' crime or 'cyber-dependent' crime. Cyber-enabled crimes are traditional crimes facilitated by the use of computers, such as fraud perpetrated through computer scams (Cross 2020). Cyber-dependent crimes are those crimes that would not exist without the technology, such as a state seeking to crash another state's internet structure (Perlroth 2021). Another useful classification is the one devised by Gordon and Ford (2006) who divided activities into Type I and Type II offences. Type I cybercrimes are crimes which are more technical in nature, for example, implementing malware attacks designed to disrupt a business by destroying its database (Falk and Brown 2022), or the activities of the 'hacktivist,' someone who protests against an organisation's actions or policies by orchestrating a denial of service (Sarre, Lau and Chang 2018). Type II cybercrime is crime that relies on human contact rather than technology, for example, fraudulent financial transactions, identity theft, romance scams, ransom attacks, theft of electronic information for commercial gain, drug-trafficking, money-laundering, aberrant voyeuristic activities, image-based sexual abuse, harassment, stalking and other threatening behaviours (Sarre, Lau and Chang 2018; Cross, Holt and O'Malley 2022). While these sorts of activities have traditionally been classified as criminal, they are now so much easier to pursue with digital technologies. Moreover, they involve far less risk of capture by local authorities (often on the other side of the world), and far less danger of physical violence which would accompany, for example, a street robbery (Sarre 2022).

Today's criminals can commit cybercrime without the need for high-level technical skills. The internet can, itself, assist, with 'do-it-yourself' malware kits, for example, available in online forums and the dark web. The borderless nature of the internet means that potential victims of cybercrime can be targeted from thousands of miles away, making law enforcement not only challenging, but, in some instances, impossible (Perkins and Howells

2021). Cybercrime is thus an escalating problem for national and international police and global security agencies.

Policing cybercrime

Tackling cybercrime is a difficult task. There are a number of factors that militate against effective crime prevention in this domain.

The first is the difficulty associated with jurisdictional boundaries. No other field of criminality finds international borders more permeable than they are in cyber criminality (Holt 2018, p. 141). It is exceedingly problematic for police or security agencies in one nation to assume control over an investigation in another nation, especially if the other nation denies that the crime emanated from within their country.

The second is the limited expertise of law enforcement when pitted against some of the best information-technology minds in the (ill-gotten gains) business (Holt 2018, p. 144). Moreover, just when the state's well-resourced teams catch up, capacity-wise, cybercrime operatives shift into another form of opaque and lawless territory.

The third factor is the rising cost of enforcement in dollar terms. Resourcing high-tech crime abatement is an expensive task, especially when there are often other more highly visible and localised calls upon the law enforcement budget (Holt 2018). True, in March 2022, the Australian Government allocated A$9.9 billion over 10 years to the Australian Signals Directorate to deliver a Resilience, Effects, Defence, Space, Intelligence, Cyber and Enablers package, the largest ever investment in Australia's intelligence and cyber capabilities (MinterEllison 2022, p. iii), and significant budgetary inputs to fight terrorism (Grattan 2015). However, there is no guarantee that government funding will ever be adequate to meet the growing demand for prophylactic measures, especially given the highly versatile and transitory nature of the phenomenon.

When one considers the above factors, it should come as no surprise that, in a time of fiscal restraint, there is a general reluctance of governments to do all of the heavy lifting. Other resourcing is needed beyond the capability and capacity of formal police forces. Fortunately, the demand is being addressed enthusiastically by a resource that is amenable to the task at hand: the private sector.

The private sector and cybercrime prevention

A great deal of the responsibility of policing the world of cybercrime has shifted away from governments to the private realm (Sarre and Prenzler 2021; 2023). On the one hand, this is a good thing: the private sector is well-resourced and ready to participate in this exercise of supplementation. Indeed, during the pandemic, the private sector was enjoined to develop the Covid-safe App and a Quick Response (QR) code regime both of which were purchased by the Australian government to assist with contact tracing. Moreover, the private sector's prophylactic measures such as multi-factor authentication of internet users and other identification software capable of thwarting cybercrime have been embraced enthusiastically by governments, too. On the other hand, the private sector can be self-serving and has been accused of being more beholden to the protection of its shareholders' interests than to the common weal (Prenzler & Sarre 2017). Former Australian Prime Minister Malcolm Turnbull offered the following by way of explanation and caution:

> If we are to fully realise the social, economic and strategic benefits of being online, we must ensure the internet continues to be governed by those who use it—not dominated by governments. Equally, however, we cannot allow cyberspace to become a lawless

> domain. The private sector and government sector both have vital roles to play. (Australian Government 2016, p. 2)

The foundations have nevertheless been laid for a strong level of cooperation between governments and private companies in facing the threats that continue to rear their heads in cyberspace. This trend goes hand in hand with private sector security cooperation that has operated under the aegis of government agencies for years and across most nations of the world in crime prevention more generally (Prenzler and Sarre 2022).

The following section outlines particular fields of endeavour where public and private crime prevention cooperative efforts and formal public / private policing partnerships have played a role (and continue to do so) in meeting the task of preventing or forestalling cybercrime– particularly in response to the risks created by the coronavirus pandemic. As can be seen, there are mixed messages that emerge from these examples in terms of potential over-reach not only of the private sector, but the public sector as well.

Metadata retention in telecommunications

Key to the way in which governments have sought to target cybercrime is the shift to accessing of digital data through what is referred to as 'metadata retention' (Branch 2014; Fernandes and Sivaraman 2015; Sarre 2017a). This strategy relies heavily upon the cooperation of the private telecommunications sector (Australian Parliament 2017). In order to frustrate and block those who would orchestrate organised crime, or who would perpetrate violence in the name of some particular ideology, governments now have the capacity to keep track of metadata by enlisting the compliance of private sector telecommunications companies (Kowalick et al. 2018).

In 2015, new laws came into force in Australia requiring telecommunications service providers to retain and store their metadata (normally, call data, SMS text data and IP addresses) so that the information remains available for analysis by crime fighters and anti-terrorism strategists (Gal 2017). The vehicle for the change in Australian policy was the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth.). The legislation circumvented any objection by the public that, contractually, their metadata information was private between them and their telecommunications provider (Sarre 2018). The new laws were not universally welcomed, however.

> Access to private communications records is already out of control in Australia, with telecommunications regulator the ACMA [the Australian Communications and Media Authority] reporting 580,000 warrantless demands in the last financial year. … But in the few years I've been working up close to government, I've learned one important lesson: Governments cannot be trusted. This government, the one before it, the one that will come after it. (Ludlam 2015)

The jury is still 'out' on whether this legislation has had the effect its designers had intended, but discussion of its use and effect has gone somewhat into abeyance (Sarre 2017b).

Surveillance tools

Visual imaging has played an important role in modern policing and the private sector has been willing and able to assist in the burgeoning market that provides the tools of surveillance. In retail shops and market precincts, for example, closed-circuit television (CCTV) has become seemingly indispensable, with widespread business support for its potential value as a means of crime reduction (Prenzler and Sarre 2012). Another innovation is the ability of surveillance tools such as facial recognition 'search' software to allow police, building owners, sportsground managers and retail proprietors (to name a few) to watch,

count and identify people moving past a certain point. Such systems are capable of tracking people not only by their facial features but by their wearing certain distinctive clothing, or walking with a distinctive gait, which is very helpful in search and rescue situations, but also in following up matters pertaining to the commission of a crime (Sarre 2020).

In the not-too-distant past, the market for these tools was limited by the size of the investment required to install and use the technology. Over the last decade, however, advances in camera technological capacity, including storage of data, have been phenomenal (Sarre 2015). These advances bring with them opportunities for public authorities and private entities to use digital data in innovative ways to manage and respond effectively to crises, crime risks and risks to property. These innovations continue to inform surveillance in cyberspace as well. Digital information can be traced and tracked with the sophisticated tools developed by privately-based cyber sleuths (Kowalick et al. 2018).

Concerns regarding the tools of cybercrime prevention

In the fight against cybercrime, however, there is good reason for apprehension. There are concerns regarding the invasion of privacy and the intrusiveness exercised by those who engage in data collection, whether instructed by governments to catch people flouting pandemic lock-down laws, or by private businesses seeking to limit commercial losses (Prenzler and Sarre 2017). These concerns include the ability of the owners of data to prevent 'leakage', namely, to forestall its spreading to a wider audience or the sale of private data for marketing purposes.

Concerns about dubious ethical practices and the regularity of instances of 'over-reach' by private companies were heightened by the March 2018 revelations that the information company Cambridge Analytica had manipulated and exploited the data of more than 80 million Facebook user profiles (Manokha 2018). This helped to facilitate the targeting of American voters with strategic electronic interruptions ahead of the 2016 United States election. Just forty-six days later, Cambridge Analytica announced it would close its doors. So, too, did its parent company, SCL Elections. Facebook admitted that it was (unwillingly and unwittingly) complicit in this clear breach of privacy.

> It might seem inherently incompatible with democracy for that knowledge to be vested in a private body. Yet the retention of such data is the essence of Facebook's ability to make money and run a viable business … Maybe the internet should be rewired from the grassroots, rather than be led by digital oligarchs' business needs. (Joseph 2018)

According to Manokha (2018), there is a new era of 'surveillance capitalism' brewing.

> The outcry against Cambridge Analytica has not attempted to sanction, nor even to question, the existence of digital platforms and other actors which depend on the ever more extensive acquisition and monetisation of personal data. If anything, the Cambridge Analytica story has unintentionally contributed to the further normalisation of surveillance and the lack of privacy that comes with being an internet user nowadays. Even the web pages of the sites that broke the story (The Observer and New York Times) allow dozens of third-party sites to obtain data from the browser of the user accessing the articles. It was 75 and 61 sites, respectively, last time I checked … (Manokha 2018)

The case of Cambridge Analytica provides a sobering reminder of why the relationship between government policing agencies and the private sector needs to be kept under constant scrutiny (Holt 2018, p. 153). Indeed, modern societies struggle to find an acceptable balance between the rights of their citizens to enjoy freedom from the prying eyes of government (and the private security businesses enjoined by governments to assist them), and the

legitimate interests that the state might have in monitoring them. In July 2015, the then Australian Communications Minister (and later Prime Minister) Malcolm Turnbull expressed the challenge in this way.

> [W]e need to recognise that getting the balance right is not easy (not least because the balance may shift over time) and we are more likely to do so if there is a thoughtful and well-informed public debate − weighing up the reality of the national security threat, the effectiveness of particular proposed measures and then asking whether those measures do infringe on our traditional freedoms and if so whether the infringement is justifiable. (Turnbull 2015)

It is appropriate to turn attention to address the challenge posed by the former Communications Minister.

Getting the balance right

An appropriate equilibrium must be struck between forestalling cybercrime using all available electronic and disruptive means (public and private), while not unduly curtailing the legitimate rights to privacy that citizens in modern democracies currently expect to enjoy. How much government surveillance is acceptable? What controls should society employ over the private sector to monitor its engagement in cyber surveillance? What degree of intrusion is acceptable? There are no easy answers, especially given that modern society appears uncertain about what levels of privacy its citizens demand, and the extent to which its citizens trust private operators and governments to manage their private data.

On the one hand, there is the view that we should safeguard strictly the privacy of the personal data held by governments and private companies, given that digital data can spread worldwide in a matter of seconds, or can be hacked, or can be used to target our potential voting preferences. On this view, we should be very cautious of any covert surveillance that allows an emboldening of private and governmental agencies to spy upon the legitimate activities of those whom they (or any other authorities) deem ‘undesirable.’

On the other hand, there is a strong sense that citizens’ lives are enhanced by having a ready supply of data available to anyone who wishes to access it. The new generations of digital users appear to be ambivalent about how much privacy they are willing to sacrifice in the rush to maintain contemporaneous contact with the world (Sarre 2014a). Access to internet sites and messaging services such as Instagram, Facebook, Facetime, WhatsApp, Viber, and Tango, for example, has enhanced private communication channels across the globe. They provide instantaneous and useful information as demonstrated during the pandemic when health advice was disseminated widely on the Internet. Each can act as a safety and protection tool, too, when, say, a user is lost, or fearful, or has become a victim of crime.

Experience has shown that private companies, however, cannot be trusted unequivocally to deal with our data in a manner that befits our privacy, and meets our expectations (Gal 2017). In the wake of two high-profile data breaches in October 2022 (Optus and Medibank Private), the Australian Government introduced legislation that exponentially increases the financial penalties entities face for allowing cybercriminals to expose these entities to repeated or serious privacy breaches. Attorney-General Mark Dreyfus introduced the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth.) which significantly increased the existing maximum penalty to whichever is the greater of an A$50 million fine; three times the value of any benefit obtained through the misuse of information; or 30 percent of a company’s adjusted turnover in the relevant period (ACSM 2022).

But government intrusions can be problematic too. In September 2021, the Australian Federal parliament passed the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021

(Cth.) which introduced new law enforcement powers to combat online crime. With the support of the, then, Labor opposition, the government sought to create new police powers to spy on criminal suspects online, disrupt their data and take over their accounts (Kantor and Kallenbach 2021). The Bill sought to create three new types of warrants to enable the Australian Federal Police and Australian Criminal Intelligence Commission to surveil Australians operating in networks suspected of committing cybercrimes. Data disruption warrants need to be 'reasonably' necessary and proportionate, and account takeover warrants need to specify the types of activities proposed to be carried out.

The Bill became law despite concerns about the low bar regarding who can authorise a warrant, and amidst allegations that the government failed to implement all the safeguards recommended by the bipartisan Joint Committee on Intelligence and Security which had reviewed the Bill (Karp 2021). Indeed, under the Act it is an offence for the media to engage in an unauthorised disclosure about a specific data disruption or account takeover, although there is a public interest exception for any person working in a professional capacity as a journalist.

Opponents of the Act argued that the legislation further erodes privacy rights, and that the targets of the new law could be broader than organised cybercrime networks and extend to civil and political activists (Kantor and Kallenbach 2021). Only time will tell how effective these new provisions will be and whether these concerns are realised.

Is There a Way Through the Maze?

To my mind, and based upon the evidence presented in this chapter, there is a way through this dilemma if private sector operatives and government security agencies and police pursue the adoption of the following policy options:

Policy option 1

This option seeks to determine what we as a society want and expect from cyberspace technology. This means that citizens need to decide what they can and cannot abide with the innovations that arise from technology, and how much they are prepared to sacrifice in the privacy versus connectedness dichotomy.

> [This] means more innovative forms of public debate. And it means that the most influential institutions in this space – …governments, technology firms and national champions – need to listen and experiment with the goal of social, as well as economic and technological, progress in mind. (Davis and Subic 2018)

Policy option 2

This option requires appropriate rules to be put in place and financed accordingly. These rules need to ensure that we can enjoy the benefits of the digital age without bringing us closer to a 'surveillance society' in which our every move is monitored, tracked, recorded, and scrutinized by the governments and private interests (Rodrick 2009). Nations should build in more safeguards as the technology becomes more widespread and spend the required money to keep them going.

Policy option 3

This option entails encouraging and adopting governmental guidelines. The Australian experience on this front is worth noting. On 8 May 2017, the Australian Government tabled the Productivity Commission's *Data Availability and Use Inquiry* (Australian Government 2018). The Inquiry made 41 recommendations designed to shift from policies based on risk avoidance towards policies based on value, choice, transparency and confidence in the

digital. A year later, on 1 May 2018, the government committed to establishing an office of the National Data Commissioner, introducing legislation to improve the sharing, use and reuse of public sector data while maintaining the strong security and privacy protections the community expects, and introducing a Consumer Data Right to allow consumers of data to share their usage with private service competitors and comparison services. The government has enshrined in legislation that data sharing and release is only for authorized for specified purposes (such as informing and assessing government policy and research and development with public benefits), and provided that data safeguards are met (Flannery 2019). Today the Office of Australian Information Commissioner exists. It is its role to monitor breaches of all forms of privacy.

Policy option 4

This option involves engagement with the private sector, but being suitably wary of its power and motives. Policymakers should be on guard to ensure that the private sector is thoroughly accountable for its cybercrime prevention efforts. Private corporations are being trusted with vast amounts of sensitive personal data that will be generated as they 'police' the internet. But there are some commentators who are not confident that this trust is well-placed.

> There are … serious unintended consequences that may result from the various extralegal measures employed by industry and corporate entities. Specifically, they have no legal or constitutional remit to enforce national laws or the interests of any one country. Industrial involvement in transnational investigations … may lead some to question whether they have overstepped their role as service providers into order maintenance based on their economic interests only. (Holt 2018, p. 152)

Policy option 5

This option entails engagement with all sectors to adopt practices of self-policing. Policymakers should ensure that the right incentives are in place to enjoin those entities that are vulnerable to cybercrime to act in their own self-interest and put in place their own shields from potential threats (Prenzler and Sarre 2022). This call has been referred to as 'responsibilisation' (O'Malley 2009). An example is the 2022 code put in place by the Australian Communications and Media Authority (ACMA). All companies (typically communications and broadcasting companies) that are required to be licensed by ACMA must now do all in their power to trace, identify and block SMS scam messages and to publish information on how to report any scams (ACMA 2022). The government has also expanded the rules required of businesses by the *Security of Critical Infrastructure Act 2022* (Cth), which became effective from 8 July 2022. Sectors defined as critical infrastructure (originally electricity, gas, water and ports) have been expanded to include businesses associated with communications, data storage or processing, financial services, healthcare and medical providers, along with sectors that deliver services such as higher education and research, food and grocery, transport, space technology, and the defence industry. Businesses and companies within these sectors are required to alert the Australian Cyber Security Centre within 12 hours of any cyber-attack if it significantly impacts their operations, and all other incidents must be reported within 72 hours.

Allied examples of responsibilisation include firms and individuals being asked to, and taking responsibility for, raising awareness of the possibilities of scams, training of staff, and target-hardening.

Conclusion

Police have a role in ensuring that cyber-space is not a lawless domain, but their resources devoted to global crime prevention are limited. They cannot go it alone especially in a post-

pandemic world where global communications are far more expansive and intrusive than ever before. That being the case, the private sector has been, and will continue to be, co-opted. Great trust between public and private agencies has been developed in relation to prophylactic measures, and that trust is set to develop.

However, given the excesses of some corporate entities, particularly in the processing and storage of digital data records, governments cannot adopt a 'hands-off' approach and allow the private sector free rein in their quest to defeat cybercrime (Sarre 2014b). It is imperative that governments regulate and monitor the interventions by the private sector into citizens' daily lives, even if it is done in the name of cyber security, lest these interventions leave people more vulnerable to policy over-reach and breaches of privacy. Hence, governments must develop a clear over-arching framework to require compliance of private owners of surveillance tools and data managers in the same way as controls (such as codes of conduct) are in place to protect the security of government-collected data.

Governments cannot afford to get this wrong. Our future security depends upon the decisions we make today regarding the strategies we need to adopt to reduce the impact of cybercrime in the years ahead that, inevitably, may entail new forms of digital responses to the latest pandemics.

References

Australian Communications and Media Authority (ACMA). 2022. 'New Rules to Fight SMS Scams', Australian Communications and Media Authority, https://www.acma.gov.au. Accessed: 12 July 2022.

Australian Competition and Consumer Commission (ACCC). 2022. 'Scams robbed Australians of more than $2 billion last year', Canberra: Australian Competition and Consumer Commission, https://www.accc.gov.au/media-release/scams-robbed-australians-of-more-than-2-billion-last-year Accessed: July 4 2022.

Australian Crime Commission (ACC). 2015. *Organized crime in Australia report*. Canberra: Commonwealth of Australia.

Australian Cyber Security Centre. 2017. *Australian Cyber Security Centre 2017 Threat Report*. https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf Accessed: 20 February 2019.

Australian Cyber Security Magazine (ACSM). 2022. Australian Government to Increase Data Breach Penalties, *Australian Cyber Security Magazine*, 24 October. https://australiancybersecuritymagazine.com.au/australian-government-to-increase-data-breach-penalties/ Accessed: 17 January 2023.

Australian Government. 2016. *Australia's Cyber Security Strategy.* https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf Accessed: 20 February 2019.

Australian Government. 2018. *New Australian Government Data Sharing and Release Legislation,* Issues Paper for Consultation. Canberra: Department of Prime Minister and Cabinet.

Australian Parliament. 2017. *Review of the implementation period of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2014,* 13 April. Canberra: Joint Parliamentary Committee on Intelligence and Security.

Branch, Phillip. 2014. 'Surveillance by metadata'. *Issues* 109 (December): 10-13.

Broadhurst, Roderic and Chang, Lennon Yao-Chung. 2013. 'Cybercrime in Asia: Trends and challenges' in *Handbook of Asian Criminology* Liu, Jianhong, Hebenton, Bill and Jou, Susyan (eds.), 49-63. New York: Springer.

Chang, Lennon Yao-Chung. 2012. *Cybercrime in the Greater China Region: Regulatory Responses, and Crime Prevention Across the Taiwan Strait* Cheltenham: Edward Elgar Publishing.

Cross, Cassandra, Holt, Karen and O'Malley, Roberta Liggett. 2022. '"If U Don't Pay they will Share the Pics": Exploring Sextortion in the Context of Romance Fraud', *Victims & Offenders: An International Journal of Evidence-based Research, Policy, and Practice* https://doi.org/10.1080/15564886.2022.2075064 Accessed: 23 September 2022.

Cross, Cassandra. 2020. '"Oh we can't actually do anything about that": The problematic nature of jurisdiction for online fraud victims' *Criminology and Criminal Justice*, 20(3), 358-375.

Davis, Nicholas and Subic, Aleksandar. 2018. 'Hope and fear surround emerging technologies, but all of us must contribute to stronger governance', *The Conversation*, 18 May. https://theconversation.com/hope-and-fear-surround-emerging-technologies-but-all-of-us-must-contribute-to-stronger-governance-96122 Accessed: 1 February 2019.

Economist. 2017. 'Data is the new oil' *The Economist*, 6 May. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data Accessed: 17 January 2023.

Falk, Rachael and Brown, Anne-Louise. 2022. 'Exfiltrate, Encrypt, Extort: The Global Rise of Ransomware and Australian's Policy Options', *Journal of the Australasian Institute of Policing* 14(2) 29-37.

Fernandes, Clinton and Sivaraman, Vijay. 2015. It's only the beginning: Metadata retention laws and the internet of things *Australian Journal of Telecommunications and the Digital Economy*, 3(3). http://telsoc.org/ajtde/index.php/ajtde/article/view/21 Accessed: 1 February 2019.

Flannery, Angela. 2019. *Public Sector Data: The Proposed Data Sharing and Release Act and implications for governments.* http://www.mondaq.com/article.asp?article_id=772966&signup=true Accessed: 1 February 2019.

Gal, Un. 2017. 'The new data retention law seriously invades our privacy – and it's time we took action', *The Conversation* 16 June. https://theconversation.com/the-new-data-retention-law-seriously-invades-our-privacy-and-its-time-we-took-action-78991?sa=pg2&sq=metadata&sr=1 Accessed: 1 February 2019.

Gordon, Sarah and Ford, Richard. 2006. 'On the definition and classification of cybercrime', *Journal of Computer Virology*, 2, 13–20.

Grabosky, Peter. 2007. *Electronic Crime.* New Jersey: Prentice Hall.

Grattan, Michelle. 2015. '$131 million for companies' metadata retention in budget boost to counter terrorism', *The Conversation* 12 May, https://theconversation.com/131-million-for-companies-metadata-retention-in-budget-boost-to-counter-terrorism-41637 Accessed: 1 February 2019.

Holt, Thomas J. 2018. 'Regulating Cybercrime through Law Enforcement and Industry Mechanisms', *The Annals of the American Academy of Political and Social Science* 679 (1), 140-157.

Joseph, Sarah. 2018. 'Why the business model of social media giants like Facebook is incompatible with human rights' *The Conversation*. 3 April. https://theconversation.com/why-the-business-model-of-social-media-giants-like-facebook-is-incompatible-with-human-rights-94016 Accessed: 1 February 2019.

Kantor, Susan and Kallenbach, Paul. 2021. 'How might the new Identify and Disrupt laws impact you?' https://www.minterellison.com/articles/how-might-the-new-identify-and-disrupt-laws-impact-you Accessed: 1 July 2022.

Karp, Paul. 2021. 'Australian powers to spy on cybercrime suspects given green light' *The Guardian*, 25 August 2021.

Kowalick, Phil, Connery, David and Sarre, Rick. 2018. 'Intelligence-sharing in the context of policing transnational serious and organized crime: a note on policy and practice in an Australian setting' *Police Practice and Research: An International Journal* 19(6), 596-608.

Ludlam, Scott. 2015. 'Data retention: We need this Opposition to oppose' *ABC The Drum,* 27 February http://www.abc.net.au/news/2015-02-27/ludlam-we-need-this-opposition-to-oppose/6269504 Accessed: 1 February 2019.

Manokha, Ivan. 2018. 'Cambridge Analytica's closure is a pyrrhic victory for data privacy' *The Conversation,* 3 May. https://theconversation.com/cambridge-analyticas-closure-is-a-pyrrhic-victory-for-data-privacy-96034 Accessed: 1 February 2019.

McGuire, Mike and Dowling, Samantha. 2013. *Cybercrime: A review of the evidence: Summary of key findings and implications*. Home Office Research Report 75. London: Home Office, October.

MinterEllison. 2022. *Perspectives on Cyber Risk*, https://www.minterellison.com/articles/perspectives-on-cyber-risk-new-threats-and-challenges-in-2022 Accessed: 1 July 2022.

O'Malley, Pat. 2009. 'Responsibilisation,' in Wakefield, Alison and Fleming, Jenny (eds), *Sage Dictionary of Policing*, 277-279, London: Sage Publications.

Perkins, Roberta C. and Howell, C. Jordan. 2021. 'Honeypots for Cybercrime Research' in Lavorgna, Anita and Holt, Thomas J. (eds.), *Researching Cybercrimes,* 233-261, Geneva: Springer Nature.

Perlroth, Nicole. 2021. *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race,* London: Bloomsbury.

Prenzler, Tim and Sarre, Rick. 2012. 'Public-Private Crime Prevention Partnerships' in Prenzler, T. (ed). *Policing and Security in Practice: Challenges and Achievements,* 149-167, Basingstoke, Hampshire: Palgrave Macmillan.

Prenzler, Tim and Sarre, Rick. 2017. 'The security industry and crime prevention', in Prenzler, T. (ed) *Understanding crime prevention: The case study approach,* 165-181, Samford Valley, Queensland: Australian Academic Press.

Prenzler, Tim and Sarre, Rick. 2022. 'Facilitating Best Practice in Security: The Role of Regulation' in Gill, M (ed.), *Handbook of Security,* 777-799, Houndmills: Palgrave-Macmillan.

Rodrick, Sharon. 2009. 'Accessing telecommunications data for national security and law enforcement purposes' *Federal Law Review* 37(3): 375-415.

Sarre, Rick and Prenzler, Tim. 2021. 'Policing and security: Critiquing the privatisation story in Australia' in Birch, Philip, Kennedy, Michael and Kruger, Erin (eds.) *Australian Policing: Critical issues in 21st century police practice*, 221-233, New York, NY: Routledge.

Sarre, Rick and Prenzler, Tim. 2023 forthcoming. 'Cyber Space Crime Prevention Partnerships in Blackstone, Erwin A., Hakim, Simon and Meehan, Brian. (eds), *Handbook on Public & Private Security,* New York: Springer.

Sarre, Rick, Brooks, David Jonathan, Smith, Clifton L. and Draper, Rick. 2014. 'Current and Emerging Technologies Employed to Abate Crime and to Promote Security', in Arrigo, Bruce A. and Bersot, Heather Y. (eds.) *The Routledge Handbook of International Crime and Justice Studies*, 327-349, New York: Routledge.

Sarre, Rick, Lau, Laurie and Chang, Lennon. 2018. 'Responding to Cybercrime: Current Trends' *Police Practice and Research: An International Journal,* 19(6), 515-518.

Sarre, Rick. 2014a. 'The use of surveillance technologies by law enforcement agencies: what are the trends, opportunities and threats?' in Pływaczewski, Emil W. (ed.), *Current Problems of the Penal Law and Criminology,* 755-767, Białystok, Poland: Temida Publishing House.

Sarre, Rick. 2014b. 'National security gags on media force us to trust state will do no wrong', *The Conversation*, 26 September 2014. https://theconversation.com/national-security-gags-on-media-force-us-to-trust-state-will-do-no-wrong-32103 Accessed: 20 July 2022.

Sarre, Rick. 2015. 'Eyes in the Sky', *Drone Magazine*, Issue 1, 48-51.

Sarre, Rick. 2017a. 'Metadata retention as a means of combatting terrorism and organized crime: a perspective from Australia' *Asian Journal of Criminology* 12: 167-79.

Sarre, Rick. 2017b. 'The surveillance society: a criminological perspective' in Viano, Emilio C. (ed.) *Cybercrime, Organized Crime, and Societal Responses: International Approaches,* 291-300, New York City: Springer.

Sarre, Rick. 2018. 'Revisiting metadata retention in light of the government's push for new powers' *The Conversation*, 8 June 2018. https://theconversation.com/revisiting-metadata-retention-in-light-of-the-governments-push-for-new-powers-97931 Accessed: 1 March 2020.

Sarre, Rick. 2020. 'Facial recognition technology is expanding rapidly across Australia. Are our laws keeping pace?' *The Conversation,* 10 July 2020. https://theconversation.com/facial-recognition-technology-is-expanding-rapidly-across-australia-are-our-laws-keeping-pace-141357 Accessed: 1 March 2020.

Sarre, Rick. 2022. 'Policing cybercrime: Is there a role for the private sector?' in Eterno, John A., Stickle, Ben, Peterson, Diana Scharff and Das, Dilip K. (eds.) *Police Behavior, Hiring and Crime Fighting,* 217-227, New York, NY: Routledge.

Turnbull, Malcolm. 2015. 'Magna Carta and the rule of law in the digital age' Speech to the Sydney Institute, Sydney, 7 July. https://www.malcolmturnbull.com.au/media/speech-to-the-sydney-institute-magna-carta-and-the-rule-of-law-in-the-digit Accessed: 18 January 2021.

Final points on this submission: a way forward

The phenomenon of cybercrime is set to continue apace. Globalisation will continue to expand, and, with the internet's highly decentralised structure of connectivity and communication, globalisation will continue to accept and promote anonymity. Thieves can be working tens of thousands of kilometres from their victims. Moreover, by virtue of the borderless nature of the internet, thieves can pretend that they are in the same location as the victim who is none the wiser to the ruse.

Moreover, as Grabosky and Smith observed a quarter of a century ago, "crime follows opportunity." Hence, electronic commerce will continue to facilitate the transactions of the dark-web illicit markets such as the Silk Road drug markets, the distribution of malicious content, and ransomware. Other criminal elements will continue to engage in hacking or phishing for unsuspecting victims, or stealing identities with ruthless and instantaneous efficiency.

Researchers will not only need to focus on the trends and issues in illicit activity but also to apply their minds and test their theories against three other recent developments that require mention (and attention) here.

1. The first is the way governments and the courts are demanding that Australian corporations take more responsibility in the cybercrime prevention task. In May 2022, the Australian Federal Court made a ruling against the Australian Financial Services Licence (AFSL) holder RI Advice, which, after several security breaches, was found to have breached the *Corporations Act (2001)* by not having adequately addressed its cyber risks. At the same time, and in harmony with this ruling, significant changes to the *Security of Critical Infrastructure Act (2018)* came into force. This Act now requires critical infrastructure asset owners and operators to demonstrate adequate and principles-based risk management for their cyber, personnel, supply chain and physical security. Under the Act, asset owners, operators and their Boards are made directly accountable for establishing and implementing a robust risk management program.
2. The second is the phenomenon observed by Harkin and Molnar of the massive rise in buying and selling security tools, which they refer to as the 'commodification of security.' An ongoing research agenda is, they assert, urgently required to bring the appropriate level of academic and social scrutiny to practices of cyber security commodification that have thus far been under-developed if not entirely lacking (Harkin and Molnar 2022).
3. The third imperative is to answer the call to build better public-private collaboration, or co-production of cyber security. At the moment these alliances are largely ad hoc and all too often caught up in commercial in confidence agreements which place them outside the gaze of policymakers and evaluators.

There is not a moment to lose.

Harkin, Diarmaid and Molnar, Adam. 2022, 'The Buying and Selling of Cyber Security Commodities', *Crime, Law and Social Change*, https://doi.org/10.1007/s10611-022-10037-y

Professor Rick Sarre, October 12, 2025