Chapter 4

Drugs and the Dark Web: The Americanisation of Policing and Online Criminal Law From an Australian Perspective

Ian J. Warren and Emma Ryan

Abstract

This chapter argues that the Americanisation of online policing has questionable impacts in Australian prosecutions involving drugs obtained and distributed through dark web cryptomarkets. The authors describe several Australian prosecutions of mid- and low-level dealers who have accessed drugs through the dark web and contrast these with the United States (US) case against the cryptomarket, AlphaBay. The discussion in this study emphasises how Australian police and courts view the relative weight of dark web activity associated with the domestic and transnational supply of illicit drugs that result in formal prosecutions. The authors suggest that large-scale forms of online and dark web police surveillance undertaken by US enforcement agencies reflect Ethan Nadelmann's (*Cops across borders: the internationalization of US criminal law enforcement*, University Park: Pennsylvania State University Press, 1993) thesis on the Americanisation of global policing through transnational communications networks. The authors then explain how key elements of transnational dark web drug supply appear to have a marginal bearing on criminal investigations into low- and mid-level traffickers in Australia, which rely on conventional surveillance tactics to identify clandestine mail pickups, physical distribution methods, and irregular money trails. However, the authors then illustrate how the Americanisation of online policing that targets high-level entrepreneurs and seeks to dismantle or eliminate dark web cryptomarkets has

Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity, 45–57

doi:10.1108/978-1-80043-866-820231004

important implications on Australian reforms aimed at enhancing online surveillance powers to target a range of crimes that are often wrongly associated with illicit drug cryptomarkets. The authors conclude by demonstrating how intensive dark web surveillance has limited direct impact on routine drug policing in Australia, with dark web communications simply another medium for facilitating the physical detection of illicit transnational drug transactions.

Keywords: Dark web; criminal trials; evidence; investigations; Australia; law

Introduction

An increasing number of criminal cases in Australia refer to the accessibility and potentially devastating effects of drugs obtained through dark web[1] cryptomarkets. The distribution of illicit drugs through the dark web serves as a supplement to conventional physical domestic and international drug markets. The significance of cryptomarkets rests with the speed of communication that can facilitate more transactions, the anonymity provided by encrypted dark web technologies, their transnational reach, the potential ease of purchasing, and the perceived superiority of the product (Barratt et al., 2014; Colman, 2023, Chapter 6, this volume). While the ease of illicit drug supply through cryptomarkets appears to generate networks that are sometimes associated with other online crimes, including credit card fraud, dark web vending can also reduce the harms and associated illegal by-products of conventional drug markets, including the level of violence associated with street trading (Martin, 2014a, 2018; Munksgaard and Martin, 2020b). Research also indicates many dark web vendors and purchasers are involved in low- to mid-level trafficking that is not necessarily sustained, highly profitable, or global in nature (Tzanetakis, 2018b).

Such findings suggest dark web markets are substantively different from conventional drug markets. However, we demonstrate that dark web markets are a form of 'Uberisation' of drug distribution that simply speeds up the communication process between willing consumers and suppliers, while utilising rather crude methods of transportation through conventional mail systems (see Craciunescu and South, 2023, Chapter 7, this volume). In fact, many relatively innocuous forms of low-level drug trafficking service small markets of friends and risk becoming labelled by law enforcement as highly serious because they utilise the dark web for transnational drug distribution. Further, even if dark web cryptomarkets impose 'explicit market prohibitions on contract killing and child exploitation activity' (Martin et al., 2019, p. 61), law enforcement often conflates these offences, which contributes

[1]Australian legal cases use the terms 'dark web' and 'darknet' interchangeably. We adopt the term dark web in line with Gehl's (2018, p. 9) view that it helps to limit discussion to web technologies, rather than Internet technologies, such as email, that can be routed through network software to enable anonymous or encrypted communication (see also Martin et al., 2019, pp. 13–14).

to an increasing array of contentious remote (Warren et al., 2020) and undercover surveillance tactics (Bleakley, 2019). These measures can have profound impacts in reshaping police investigative procedures in the open and dark webs as well as the laws that sanction the admissibility of evidence obtained through cooperative transnational investigations involving multiple law enforcement agencies. Regulatory concerns over the seemingly impenetrable nature of advanced encryption technologies within the specific places of the dark web (Bowling and Sheptycki, 2011) potentially generate a troubling expansion of covert extraterritorial surveillance often aimed at protecting United States (US) commercial and law enforcement interests. However, these processes can also undermine individual liberty and due process in other jurisdictions (Mann and Warren, 2018; Warren et al., 2020).

Our argument demonstrates how the policing of low- and mid-level drug trafficking that uses the dark web to facilitate distribution is reliant on many physical attempts to control and eliminate illegal drug markets. We also consider how the transnational nature of illicit recreational drug supply through dark web cryptomarkets reflects two regulatory anxieties indicative of the US approach to the global war on drugs (Andreas and Nadelmann, 2006) and more recent efforts to shed light on illicit activities in the dark web (Kerr and Murphy, 2017). These developments generate two mutually reinforcing tiers of drug law enforcement that mirror and build on the conventional distinction between trafficking and use. At one level, most conventional drug enforcement activity targets the activities of low-level users and dealers at the end point of the distribution chain, through the interception of mailed packages or the laundering of the proceeds of criminal activity, who are commonly detected through conventional surveillance processes but have used the dark web to gain access to or facilitate the distribution of their product. At the higher end, law enforcement uses sophisticated and highly technical forms of surveillance to target the managers and administrators of dark web cryptomarkets. At this level, there is the greater impetus for enhanced legal powers to undertake dark web surveillance and various forms of cross-jurisdictional intelligence sharing targeting both drug and non-drug crimes and potential criminal conspiracies (Mann and Warren, 2018). These measures aim to eliminate illicit dark web cryptomarkets.

Central to these processes is the transnational scope of dark web activities. While global drug trafficking markets in the pre-Internet era generally involved some degree of transnational communication and organisation, the dark web adapts these processes to enable faster and more direct communication among geographically dispersed suppliers and consumers. This creates an interesting dimension to dark web cryptomarkets, as it is also common for many dark web vendors to avoid transactions with people in jurisdictions with enhanced surveillance of regular mail, such as Australia and the USA (Martin, 2014a; Bancroft, 2020), which is not a direct result of enhanced dark web policing. Rather, this development reflects the convergence of physical and online enforcement measures involving the interconnected nature of illicit drug distribution and cryptomarket activity.

We document several representative cases involving evidence that illicit drugs have been procured through the dark web, which are derived from a broader sample of 20 Australian legal rulings handed down between January 2018 and

November 2020 contained in the Lexis Advance Pacific subscription database. We also examine the US decisions stemming from the takedown of the AlphaBay website. Legal records reveal the types of evidence obtained by police that sustain criminal charges when illicit drug transactions have been arranged through the dark web, as well as any parallel offences raised in these scenarios (Warren, 2011). This information is useful given the limited public disclosure about police operations in dark web cryptomarkets. For example, court decisions can provide some accountability for police surveillance practices in drug investigations, given that mandated processes for documenting how and when communications interception warrants are granted to police tend to omit key information, such as the types of offences or circumstances that justify lawful interference with private digital communications (Molnar and Warren, 2020). Before outlining key themes that emerge in our sample, it is important to identify how broader developments in the Americanisation of drug and online criminal law enforcement have the potential to shape the investigative processes that lead to criminal prosecutions for activities in dark web drug cryptomarkets

The Americanisation of Drug and Online Policing

Ethan Nadelmann's (1993) landmark study of the Americanisation of modern policing shows how US law enforcement agencies used offshore liaison officers to help build the capacity of foreign law enforcement agencies to combat transnational drug trafficking. Since Nadelmann's work, these processes expanded markedly throughout Central and South America. This was largely through the establishment of bilateral treaties negotiated by the US, often accompanied by considerable US funding, which sought to build the capacity and degree of cooperation between law enforcement agencies throughout the region (Kontorovich, 2009). A common site for drug trafficking and law enforcement activity is the maritime region between South and North America, where extensive resources have been dedicated to limiting the illicit smuggling of drugs, people, and weapons into the US. Bilateral enforcement treaties commonly conferred expanded investigative and arrest powers on foreign law enforcement agents, which streamlines the transfer of evidence and suspects to face criminal charges under US law (Kontorovich, 2009). These processes enable prosecutions to proceed even if the drugs have been destroyed, there is limited evidence they were destined for the US, or if the suspects had never previously set foot on US soil (Warren and Palmer, 2015).

Bilateral treaties formalise otherwise informal agreements between domestic police agencies that shape the trajectory of transnational law enforcement cooperation (Bowling and Sheptycki, 2011, 2015). We argue two main problems stem from these developments. First, the tactics associated with general drug policing become globally fortified through a logic of zero tolerance that reflects US political, economic, and law enforcement interests. These values are then promoted as the desired approach in regional and global drug regulation (Andreas and Nadelmann, 2006). Second, specific rules, procedures, and enforcement tactics adopted by US police agencies infiltrate the law enforcement processes of

foreign police agencies. This process normalises various forms of police practice that are determined by US norms and standards. Examples include various forms of paramilitarisation and undercover surveillance activity, as well as procedures for search and seizure, evidence collection, and the apprehension and transfer of suspects in regions where treaties are in place. These processes reinforce the logic of zero tolerance, while the US subsidises the development of law enforcement approaches that seek to eliminate drug trafficking by extending these preferred ideas of appropriate police practice and the rule of law to neighbouring or partner countries. The result is the gradual Americanisation of both the laws and substantive methods for drug law enforcement, which is further prompted by the deployment of liaison officers to help coordinate and oversee these transnational operations (Nadelmann, 1993; see also den Boer and Block, 2013).

Contemporary developments in the policing of transnational online offending and dark web cryptomarkets mirror these processes in ways that build on the processes identified by Nadelmann (1993) and Kontorovich (2009). Two examples illustrate how measures led by the US to police transnational online crime can have direct impacts on the laws and law enforcement processes of other countries.

The first example involves the case of Kim Dotcom. After a request by the US Federal Bureau of Investigation (FBI) that raised allegations of systematic criminal copyright violations in the peer-to-peer file-sharing website Megaupload, Dotcom's home in Auckland was subject to the largest raid in New Zealand (NZ) policing history on the morning of 20 January 2012 (Palmer and Warren, 2013). After extensive litigation on various technical points of law, the Supreme Court of NZ in *Ortmann et al.* v. *United States of America* (2020) authorised the extradition of Dotcom and three co-accused to the US in 2020 to face 12 charges involving criminal copyright infringement and racketeering offences linked to this 'mega conspiracy' (Boister, 2017). Extradition for a single count of conspiracy to commit money laundering was denied because there were no equivalent NZ laws to deal with this US charge. While numerous legal technicalities have been examined in detail in the NZ court system, further legal review will examine procedural irregularities with some evidence that were overlooked in one of the many previous hearings (Hurley, 2020; *Ortmann et al.* v. *USA*, 2020). Ultimately, the complexity of these issues is a symptom of a broader

> extension of domestic policing power under external [US] influence and [demonstrates] how securitisation of law enforcement cooperation can remove existing domestic legal barriers and penetrate the enforcement of domestic law and order. (Boister, 2017, p. 241)

These issues extend well beyond the legality of the initial NZ police raid in January 2012 (Palmer and Warren, 2013), covering important, and highly technical, questions of criminal procedure designed to prevent the abuse of police power under NZ and US search and seizure laws, including ill-informed 'fishing expeditions' to obtain incriminating evidence (Boister, 2017, p. 233). Cases examining the NZ police raid generated proven allegations that NZ police engaged in the unauthorised and unlawful transfer of evidence to US authorities, including

documents, bank records, and digital devices such as encrypted hardware, mobile telephones, and pagers, as well as the seizure and sale of assets derived from Megaupload profits under NZ asset forfeiture and US fugitive disentitlement laws (*USA* v. *Batato et al.,* 2016). There have also been significant concerns regarding the level of potentially unlawful surveillance of Megaupload's activity by the NZ Government Communications Security Bureau (GCSB), including debate over whether these intelligence records should be disclosed to assist the defence (Boister, 2017). This has raised additional questions about the availability of human rights relief and monetary damages for alleged privacy violations by the GCSB and several other NZ government agencies (*Dotcom* v. *Attorney General*, 2020).

The economic and political fallout from this protracted investigation is extensive and highly complex. However, this saga aptly demonstrates why a more coherent approach to transnational police investigations into serious online offences is required to ensure greater procedural transparency (Bowling and Sheptycki, 2015). Equally, it illustrates why the transfer of police powers under bilateral anti-drug trafficking treaties (Kontorovich, 2009) should not automatically reshape the processes of justice administration in other nations, because existing domestic legal protections can provide meaningful accountability for transnational police activity that is otherwise missing from these cooperative arrangements, even if they are legally complex and highly protracted.

The second example involves the FBI's role in dismantling the Silk Road dark website, which raised similar problems involving transnational access to admissible evidence (Mann and Warren, 2018). Much investigative activity, in this case, targeted Ross Ulbricht, aka Dread Pirate Roberts, a US citizen who was the leading Silk Road site administrator undertaking the bulk of allegedly unlawful dark web activity from within the US. However, the FBI and US government devoted significant investigative and legal resources towards identifying and apprehending several offshore accomplices who allegedly helped with the administration of the Silk Road cryptomarket. This included Irish citizen Gary Davis, who resisted extradition for several years due to legal uncertainty over the FBI's decision to seek evidence of his connection to Ulbricht directly from the Microsoft Corporation, which owned servers in Ireland that contained online communications between the two. This case shows the difficulties associated with relying on mutual legal assistance requests with foreign governments to access digital evidence (Warren, 2015). However, the willingness of US authorities to bypass the mutual legal assistance process in the Silk Road investigation was explicitly designed to 'send an unmistakeable message' to people engaged in online offending that 'the dark web does not cast shadows long enough to protect criminals from the long arm of the law' (Department of Justice, 2019).

The evidentiary problem in the Davis case has been rectified by the Clarifying Lawful Overseas Use of Data (CLOUD) Act. This US law seeks to replace mutual legal assistance procedures for the transnational exchange of admissible evidence. It enables the US to negotiate bilateral executive agreements that enable law enforcement agencies to obtain data in the control of technology companies operating in preferred nations that can later be used as admissible evidence in

criminal trials (Daskal, 2019). Mirroring the maritime drug enforcement treaties mentioned by Kontorovich (2009), the CLOUD Act is a US-led legislative response to rectify the problems of transnational surveillance and evidence exchange that reflects US demands to shed light on the dark web through streamlined procedures (Kerr and Murphy, 2017). These executive agreements suspend the geographic constraints of criminal jurisdiction through 'a unidirectional spatial dispersal of paper rules' (Boister, 2012, p. 277) that shape the domestic laws of other nations when dealing with cooperative transnational investigations into serious online crimes. Ultimately, these processes enable the US

> to apply its own criminal laws, access extraterritorial evidence with domestically authorized search warrants and request the extradition of alleged coconspirators to face trial in the US before any other nation [has] activated its domestic jurisdiction. (Mann and Warren, 2018, p. 254)

These developments are backed by considerable scholarly support for upholding US standards of law and investigative integrity to enhance 'privacy and civil liberties' in other nations (Daskal, 2019, p. 1048). Such supportive attitudes within the US legal and scholarly fraternities are seldom open to external challenge or are usually supported by reference to vague or undocumented norms of police cooperation and intelligence exchange operating independently of a coherent body of transnational procedural law or selectively applied 'rule with law' (Bowling and Sheptycki, 2015). In other words, although it is reasonable to argue that other nations may not be offended by foreign surveillance to investigate serious transnational crime (Kerr and Murphy, 2017) or the establishment of informal agreements allowing for undetermined levels of transnational intelligence or evidence exchange with any number of countries to police various dark web crimes, these processes must ultimately remain subject to domestic laws and procedures that respect due process and territorial sovereignty (Ghappour, 2017). In the next two sections, we examine whether these developments influence domestic Australian prosecutions involving evidence of drugs obtained through the dark web and how these patterns might be mirrored in other large-scale investigations led by the US aimed at dismantling dark web cryptomarkets.

Australian Drug and Dark Web Cases

We have traced 20 reported cases decided between January 2018 and November 2020 that mention drugs obtained via the dark web by a convicted or sentenced person in the Lexis Advance Pacific subscription database, which documents significant rulings involving points of law, procedure, or sentencing in Australia. This database is also linked to equivalent databases spanning the South Pacific, the USA, and the UK. The only specific dark web cryptomarkets mentioned in our sample are AlphaBay (*North* v. *DPP* (Cth) [2020], para. 8; *R* v. *Grey*, 2020) and Dream Market (*R* v. *Azabal*, 2019, para. 25). No specific vendors are mentioned in any of the rulings. Each prosecution appears to be based on evidence

obtained through conventional drug policing methods, including the surveillance of incoming mail, questionable financial and banking transactions, or other behaviour indicative of low-level drug trafficking. This confirms the findings of Munksgaard and Martin (2020b), which indicate much illicit drug trafficking facilitated through the dark web in Australia is of low- to mid-level frequency and involves moderate quantities of illicit drugs, financial sums, and degrees of organisational complexity. No reported Australian cases involve the takedown of a dark web drug cryptomarket, although Australian law enforcement agencies have been involved in transnational investigations involving child exploitation material (Bleakley, 2019). Evidence of dark web activity has been used by two suspects to conceal their identities in the hope of avoiding serious charges, including the planning of extremist violence and large-scale social disorder (*DPP* v. *Noori*, 2019; *Kennedy* v. *R*, 2018). In addition, Bitcoin has been used to purchase credit card details to commit frauds (*Re Abaker*, 2018). A further case involves a drug conviction from dark web activity that has affected a person's ability to practice as a registered nurse (*Health Care Complaints Commission* v. *Holbrook*, 2019). One New South Wales case involved an application by the state for an interim detention order against a serious career offender with numerous prior assault and drug convictions, who purchased cannabis oil on the dark web after being diagnosed with bone cancer (*State of NSW* v. *CT* (Final), 2019).

Reported Australian cases show how the transnational supply of illicit drugs through the dark web combines the sophistication of encrypted communication to organise the transaction with manual supply via the postal system. This process is described in *North* v. *DPP* (2020, para. 7) as the 'scattergun' approach. In this case, federal prosecutors alleged that North used the dark web on two separate occasions to arrange separate shipments of no more than one ounce of MDMA each to be mailed in envelopes through circuitous routes from Europe to the UK and eventually to Perth and Melbourne, Australia (*North* v. *DPP*, 2020, para. 7). This process was intended to reduce the prospect of detection and minimise financial losses. Interestingly, North was detected when selling unspecified 'marketable quantities' of the powder that had been converted into 'pills which bore a kangaroo stamped impression very similar to the Qantas Airways logo' to an undercover federal officer working in AlphaBay (*North* v. *DPP*, 2020, para. 8). This is not likely to have been an accidental encounter, with targeted surveillance potentially leading to the undercover operation, much in the same way as the infiltration of child exploitation networks (Bleakley, 2019). This investigation produced other charges involving pill manufacturing and the failure of the suspect to reveal computer passwords to assist investigators.

Despite evidence indicating that many dark web vendors are reluctant to transact with people in Australia or the US due to the tighter surveillance of overseas mail (Martin, 2014a; Bancroft, 2020; *Gallagher* v. *Western Australia*, 2019), several cases in our sample involved the transnational supply of illicit drugs detected through the Australian postal system. For example, the Northern Territory case of *Edmonds* v. *R* (2019) involved an appeal against a six-year imprisonment term on a charge of supplying a commercial quantity of methamphetamine and less than a commercial quantity of cannabis plant material. The court found that

> the use of Bitcoin and the dark web to purchase the drugs elevated the gravity of the offending because it demonstrated a degree of sophistication (of a sort), and it gave rise to obvious and intended difficulties in detecting the activity. (*Edmonds* v. *R*, 2019, para. 28)

However, this statement was qualified by the suggestion that all attempts at supplying commercial quantities of illicit drugs involve some form of subterfuge. Hence, the use of the dark web is considered simply an extension of conventional methods for clandestine drug supply. It can also be assumed that police suspicion of illicit drug distribution led to the surveillance of Edmonds' finances. This evidence appears at the start of the ruling and indicates that over a period of one-and-a-half years, Edmonds deposited 293,195 Australian dollars (A$) into his regular bank account to purchase A$275,000 in Bitcoin, even though his annual tradesman's salary was only A$66,000. Over a subsequent three-month period, police intercepted eight packages matching the types and quantities of drugs he purchased using Bitcoin. While over 100 grams of methamphetamine and 28 grams of cannabis were intended to be distributed 'to his nominees in the Darwin area', the court recognised 'there is nothing to indicate' this level of trafficking 'involved an extensive network or high level of activity over an extended duration' (*Edmonds* v. *R*, 2019, para. 41). Edmonds successfully argued for a 14-month sentence reduction. The remainder of his imprisonment term was suspended provided he complied with parole orders requiring him to remain in the Northern Territory and enter a residential rehabilitation program with mandatory electronic monitoring and regular drug testing. This outcome was assisted by his guilty plea.

The apprehension of a person who has obtained drugs through the dark web can sometimes involve circumstantial discovery. This was the case in *R* v. *Azabal* (2019), where the illicit drugs were linked to the cryptomarket Dream Market. The suspect was discovered after another person, Murray, was arrested for possession of cocaine and MDMA at a hotel in regional New South Wales. Murray's phone records revealed he received up to 23 grams of cocaine from Azabal in small quantities over the period of a month. While on conditional bail, an international parcel addressed to Azabal containing 138.96 grams of cocaine was intercepted by Australian Federal Police, with further packages detected on a tracking app after his arrest. One of these contained 250 grams of ketamine. Azabal received a total effective prison sentence of five-and-a-half years with a non-parole period of two years and six months. This result was calibrated against five other state and federal dark web trafficking cases. The court in *Azabal* (2019, para. 25) noted that dark web trafficking is a sign of 'calculation and organisation', with the range of drugs imported in the five comparative sentencing decisions including MDMA, illegal steroids, and carfentanyl.

A final case demonstrates a more serious domestic cannabis trafficking operation involving over 600 orders estimated to be worth an annual turnover of up to A$400,000 (*R* v. *Grey*, 2020). A husband-and-wife partnership arranged the transactions on AlphaBay using the vendor name 'Weeeeeed'. The police operation also produced evidence of several international transactions involving

MDMA, 'Coke', and methamphetamine, with various quantities of these substances seized at multiple locations (*R* v. *Grey*, 2020, para. 12). Significantly, the investigation involved the tactical interception of mailed packages destined for various locations within Australia, supported by evidence of the husband's 'large scale purchase of express post parcels and lodgement of those parcels for distribution' (*R* v. *Grey*, 2020, para. 14). Once the operation was detected, police discovered 'diligent and organised records of the customer base, tracking numbers for each package used to supply the customers, and the amounts supplied' (*R* v. *Grey*, 2020, para. 9). The husband's initial sentence of nine years imprisonment for the major trafficking offence, which included terms for less serious charges, was slightly reduced because it failed to incorporate time served in pre-sentence custody. The wife's fate remains undisclosed in available court records, save for a brief reference to the forfeiture of A$308,887.23 in jointly held criminal proceeds, including 'Porsche and BMW cars' purchased through the 'trafficking and production business from their family home and two other properties', which was considered an important measure of the couple's 'lavish lifestyle from the profits they made' (*R* v. *Grey*, 2020, para. 25).

Alphabay and the US Courts

AlphaBay was a leading cryptomarket for the distribution of illicit drugs in Australia and internationally. It was also 'designed to facilitate illegal sales of malware … guns, stolen financial information, and counterfeit documents around the globe' (*United States* v. *All Monies, Funds, & Credits*, 2020, p. 2). As with Silk Road, the key to dismantling this cryptomarket involved detecting its founder and main administrator, Canadian citizen Alexandre Cazes. The FBI and US Drug Enforcement Agency engaged in several undercover transactions with vendors in AlphaBay, resulting in the purchase of controlled substances as well as 'fake identification documents and an ATM skimmer' (*United States* v. *2013 Lamborghini Aventador*, 2018, p. 9). These items were shipped to the Eastern District of California, which provided the legal basis for US authorities to exercise their investigative jurisdiction extraterritorially.

After Cazes accidentally disclosed a personal email address in an AlphaBay welcome email and password recovery instructions in December 2014, US enforcement agents began remotely monitoring some of his dark web activities. In 2017, US agencies worked closely with the Royal Thai Police, which obtained a warrant to search Cazes' home in Bangkok. This resulted in the seizure of a laptop containing direct links to the 'Admin' account controlling AlphaBay and related financial information from sales commissions through the site. Cazes was believed to have committed suicide seven days after his apprehension in Thailand. Civil forfeiture proceedings were then commenced in California targeting the allegedly illicit finances derived from Alphabay held by Cazes and his widow. These cases reveal the economic motives behind dismantling dark web cryptomarkets.

While both forfeiture rulings were default judgments in favour of the US government, they remain the major forms of public transparency associated with this investigation. The main allegations raised at trial and on appeal suggested that

the assets identified by US authorities were 'directly traceable' to 'transactions of illegal controlled substances' conducted via AlphaBay (*United States* v. *All Monies, Funds, & Credits*, 2020, p. 12). US arguments for the right to seize these illicit funds were supported by an admission by Cazes on AlphaBay in 2014 that he sought to create 'the largest eBay-style underworld marketplace' (*United States* v. *2013 Lamborghini Aventador*, 2018, p. 6).

The US federal District Court for the Eastern District of California ordered the forfeiture of various luxury vehicles; funds in eight specified bank accounts; properties owned by Cazes in Thailand, Granada, Cyprus, and Antigua; unspecified amounts of Bitcoin and various other cryptocurrencies; and cash held in the names of Cazes and his wife identified through records stored in the AlphaBay servers (*United States* v. *2013 Lamborghini Aventador*, 2018). These profits were attributed to commissions charged for each transaction within AlphaBay. Cheques issued by Cazes to the governments of Grenada, St Kitts and Nevis, and various other countries where he sought to obtain citizenship when he believed he was under investigation were also forfeited (*United States* v. *All Monies, Funds, & Credits,* 2020, p. 15). The sweeping nature of these claims is similar to fugitive disentitlement actions against Kim Dotcom, which sought blanket default judgments allowing the seizure of all assets held in NZ and Hong Kong, based on allegations that Megaupload had generated US$175,000,000 from the US$500,000,000 in illegal losses it caused to legitimate copyright holders (*USA* v. *Batato et al.* 2016, 418). While the accuracy of these estimates is debateable, there is the clear financial impetus for these transnational enforcement measures to redress the economic harm experienced by the US government and legal businesses from clandestine online activity through sites such as Megaupload, AlphaBay, and Silk Road. However, even when small-scale secondary or parallel dark web cryptomarkets are detected and dismantled, new markets headed by new entrepreneurs tend to emerge in their wake (Dorn and South, 1990; Ladegaard, 2019).

Discussion and Conclusion

Our analysis demonstrates the ambiguity and complexity of Australian investigations involving drug transactions via the dark web. These developments mirror the history of drug regulation in many jurisdictions by attempting to dismantle illicit drug markets through formidable criminal penalties and asset confiscation processes (Dorn and South, 1990). The Americanisation of online surveillance and enforcement activity targets the speed and hidden nature of communications through dark web cryptomarkets and financial transactions using cryptocurrencies. However, while key legislative and enforcement responses target encrypted communications flows, our analysis shows that mid- to low-level Australian drug prosecutions where the dark web has been used generally involve conventional forms of police surveillance that focus on the physical legacies of drug dealing, such as access to mobile phone communications records, mail interceptions, irregular money trails, or evidence of lavish and unrealistic financial expenditure.

The transnational investigation of dark web cryptomarkets targets high-end entrepreneurs by stretching the territorial scope of US criminal investigative jurisdiction. Here, the Americanisation of online policing produces important regulatory anomalies that undermine efforts to ensure police investigations are open, transparent, and accountable through due process of law. The selective use of myriad domestic laws that favour particular enforcement ends, which Bowling and Sheptycki (2015) define as 'rule with law', enables US investigators to influence transnational online surveillance and drug interceptions in other jurisdictions. Only in rare cases involving high-profile entrepreneurs are these processes subject to detailed and open scrutiny, such as the protracted examination of the investigation into Kim Dotcom and his compatriots under NZ's extradition laws.

However, our analysis also suggests that dark web cryptomarkets are simply another communication tool for organizing mid- and low-level trafficking activity that is generally viewed by Australian courts as having a minor level of sophistication. In other words, only attempts to dismantle dark web cryptomarkets such as Silk Road and AlphaBay can provide meaningful inroads into the illicit transnational supply chain by tracing the relationships between site administrators and individual vendors (Tzanetakis and Marx, 2023, Chapter 10, this volume). These high-end investigations require the kinds of multilateral coordination promoted through bilateral agreements between law enforcement agencies and governments that are currently driven by the US (Mann and Warren, 2018).

These forms of enforcement cooperation might also capture mid- and lower-level dealers and users. However, none of the Australian cases we have examined contained specific reference to investigative activity concerning the dark web that might have led to an arrest or prosecution. It is also unclear how police determined whether mail to be searched was identified through routine postal surveillance or targeted interceptions derived from dark web activities. This issue requires more research given the comparative rigour of the warrant requirements for opening and reading mail under the US constitution (Desai, 2007), particularly as Australia has no individually enforceable Charter or Bill of Rights. Moreover, the lack of transparency in reporting obligations applicable to telecommunications interception warrants (Molnar and Warren, 2020) means that there could be considerable online surveillance and information exchange within Australia's police forces that also extends transnationally, yet is subject to limited public knowledge, judicial oversight, or external accountability (Bleakley, 2019).

The development of mutually compatible bilateral online investigative processes that can enhance transnational investigations into cryptomarkets builds on previous generations of agreements forged by the US (Kontorovich, 2009). This enhances the surveillance of both conventional online and dark web activity through executive agreements that reshape the rule of law in partner jurisdictions. In January 2020, the US finalised a CLOUD Act executive agreement with the UK, while negotiations with Australia proceeded throughout 2020 (Greaves and Swire, 2020). The Australian agreement is linked to proposed legislation introducing international production orders that allow Australian law enforcement agencies to directly obtain evidence from US technology companies, and 'network activity warrants' that will enable Australian investigators to seize and operate

dark web sites as clandestine honeypot sites, or 'poisoned water holes'. These powers aim to identify individual dark web users regardless of their geographic locations or the nature of their allegedly unlawful activities (Parliament of the Commonwealth of Australia, 2019–2020). Such enhanced enforcement powers are direct legacies of the difficulties US authorities faced in accessing admissible evidence against Gary Davis after the Silk Road cryptomarket takedown under mutual legal assistance procedures (Mann and Warren, 2018).

Any benefits of using the dark web to procure illicit drugs identified in the empirical literature (Munksgaard and Martin, 2020b; Tzanetakis, 2018b) are dismissed by the negative associations of its hidden nature in regulatory and law enforcement discourse (Kerr and Murphy, 2017). Concealment also offsets the very real concern that non-consensual extraterritorial law enforcement activity pioneered by US law enforcement agencies against Silk Road and AlphaBay might be frowned upon by other nations despite its noble intent (Ghappour, 2017). For example, the clear aim of Australia's recent legislative reforms is 'to better enable' federal law enforcement agencies

> to collect intelligence, conduct investigations, disrupt and prosecute the most serious of crimes, including child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassination, and the distribution of weapons. (Parliament of the Commonwealth of Australia, 2019–2020, p. 2)

Enhanced law enforcement cooperation in the South and North American regions was justified by questionable associations between illicit drug trafficking and 'the potential unlawful smuggling of people and weapons of mass destruction by terrorist organisations' (Warren and Palmer, 2015, p. 277). Similarly, intrusive and opaque surveillance powers that aim to shed light on the dark web are considered so incontrovertible as to be morally unchallengeable (Kerr and Murphy, 2017). This is because politicians and law enforcement agencies in the US commonly employ false and conflated notions of exceptional risk to justify ubiquitous surveillance and modes of evidence exchange unfettered by the technicalities associated with obtaining foreign government consent in specific investigations.

We consider that such expanded online investigative powers are symptoms of the Americanisation of online policing that evolve with minimal public discussion of alternate methods for dealing with the transnational supply of illicit drugs or other dark web activities. Such processes, and their underlying rationales, consider all dark web activity as evil due to its hidden nature. However, our analysis suggests high-end forms of dark web surveillance appear to have minimal impact on routine Australian drug policing. Indeed, the major source of dark web harm appears to be economic rather than physical or moral. It is, therefore, important to revisit the role of criminal law in this area by stripping away the emotive justifications for enhanced transnational law enforcement surveillance that characterise recent legal developments in this field.