Ian Warren

School of Humanities and Social Sciences, Deakin University, Australia.
ian.warren@deakin.edu.au

Introduction

Seeking better understanding of the relationship between criminal law and surveillance demands investigating the evolving nature of sovereignty in an era of transnational digital information flows. While territorial boundaries determine the limits of police investigative and surveillance powers under the criminal law, several recent United States (US) examples demonstrate how new forms of extraterritorial surveillance that enable police to access online communications by foreign citizens and digital information stored in offshore locations are authorized by US courts. This discussion outlines how the processes of mutual legal assistance that ordinarily govern the search, seizure and transfer of digital evidence from one jurisdiction to another are increasingly considered to undermine police efficiency, even though they protect the due process rights afforded to crime suspects under established principles of sovereignty (Palmer and Warren 2013).

After documenting the centrality of territory in limiting police surveillance in domestic criminal investigations, this discussion summarizes the legal rationales in two significant US court rulings that endorse questionable forms of extraterritorial online surveillance. These cases demonstrate the difficulties courts face in determining whether US law enforcement authorities should be able to access the communications of non-US citizens or data located in offshore servers controlled by US corporations. In particular, the counterintuitive logic of the public and private distinction that limits police surveillance powers under domestic criminal law is reconstituted to validate extraterritorial police surveillance power under US law and enhance the efficiency of transnational criminal investigations. Equivalent rationales also inform recent Australian measures requiring internet service providers (ISPs) to retain customer metadata for a minimum of two years that can now be accessed by police without a warrant. When combined, these developments highlight the profound limits of the criminal law in restricting the extraterritorial surveillance of online communications involving non-US citizens, particularly as US multinational corporations own and control most global information flows that are automatically deemed to fall within US criminal jurisdiction.

Sovereignty and Due Process

The potentially coercive impacts of law enforcement activity and the state's power to punish ensure the criminal law is more 'closely associated with sovereignty' than most other branches of law (Dubber 2006: 1288). Due process requirements, including the need for police to obtain judicial authorization to search and seize evidence in private locations, limit police investigative powers after probable cause is

established. Various non-authorized forms of police surveillance can later be scrutinized in pre-trial and trial proceedings when the admissibility of evidence is tested before a judge (Kerr 2012: 328). However, until these procedures commence, crime suspects are generally unaware that a subpoena or warrant has been issued to enable a more thorough investigation to proceed. It remains unclear whether the ‘added protection provided by warrants’ and ‘judicial oversight will improve the probability that [admissible] evidence will be discovered’ (Slobogin 2011: 329). Nevertheless, the increased mass surveillance of transnational digital communications to investigate or prevent criminal activity (Lyon 2014) is difficult to reconcile with established processes that determine when a warrantless search is permissible under the US Fourth Amendment (Kerr 2015) and equivalent provisions in other English-speaking jurisdictions. In fact, the challenges presented by global communication practices highlight many contradictions in the investigation of transnational crime through bi- and multi-lateral agreements between sovereign nations that characterize the fields of extradition law and mutual legal assistance (see Warren and Palmer forthcoming). These debates replicate the demarcations between public and private property that determine ‘reasonable ... governmental interests’ in domestic criminal investigations (Kerr 2012: 318).

The practical implications of the public and private distinction often seem arbitrary or counterintuitive. For example, a visibly enclosed area inside a privately managed sports venue might be considered public space that enables police to lawfully enter to arrest, detain or eject unruly and previously banned patrons (Warren 1995). If an off-duty police officer located on a public walkway sees a couple engaging in consensual sexual activity through a window located on private property, a prosecution for offensive public behavior can be sustained unless the couple had no intention to be viewed (*Pregelj v. Manison* 1987). These forms of ‘mono-analogical’ reasoning also apply to the legal classification of digital information. For example, when interpreting whether electronic data is public information that does not require a search warrant, US criminal and constitutional courts often draw analogies with manual information recording processes. Hence, a cell phone is considered the functional equivalent of an address book, because both enable ‘contact information of friends and associates’ to be aggregated (Milligan 2011: 1320). Similar reasoning allows police to use evidence obtained from tracking devices installed on private vehicles operated on public roads, but not while they are in private garages (Kerr 2012). Aerial photographs of open spaces on privately enclosed land or the voluntary disclosure of personal information to a third party (Rushin 2013) can also be lawfully accessed by police without a warrant. The first example is justifiable because any person with aerial surveillance capabilities can plainly see what a fence at ground level otherwise conceals. In the second, verbal or written information loses its private character when conveyed to someone else, making it accessible to anyone who asks. Such reasoning characterizes how judges determine the legality of each isolated component of a sequence of surveillance activities (Kerr 2015), rather than considering each element as part of a broader surveillance assemblage or ‘mosaic’ that can reveal important details about an individual’s habits, movements, activities, or opinions (Cohen 2015).

Cases involving retaliatory prosecutions for allegations of state crime or online espionage by whistleblowers (Rothe and Steinmetz 2013) present several additional challenges for established principles of territorial sovereignty. US Private Chelsea Manning was ultimately sentenced to a 35-year prison term under US military law for his role in unlawfully disclosing classified information and video footage documenting the killing of civilians in the Iraq war (Hardy and Williams 2014). Yet, the ongoing investigation into Julian Assange and many others associated with WikiLeaks as well as the subsequent activities of Edward Snowden reveal the fundamental paradox between global online communication practices and the role of territory as the primary method of constraining law enforcement surveillance under the criminal law. This paradox has a long history, dating back at least to ‘the universal establishment of a cheap letter post and of the electric telegraph’ (Cornwall-Lewis 1859: 5), which created many new opportunities for transnational crime that remained the primary responsibility of national police agencies to investigate and prosecute. Rather than developing a neutral transnational criminal law and enforcement structure, cooperative bi- and multi-lateral extradition and mutual legal

assistance treaties establish standards for the collection and transfer of crime suspects and evidence between independent sovereign nations. These commonly retain domestic warrant requirements in each jurisdiction and increasingly appear ill-equipped to accommodate the ability of police agencies to access and use digital communications records in complex criminal investigations (Warren and Palmer forthcoming; Palmer and Warren 2013; Brenner and Schwerha 2002).

Legal Justifications for Mass Dataveillance

In 2011, the US Federal District Court for the Eastern District of Virginia authorized a subpoena enabling US law enforcement agencies to access the ‘name, address, telephone connection records, records of session times and durations, length and type of service used, telephone number or temporarily assigned network address and method of payment’ (*In Re Application for the USA for an Order Pursuant to 18 U.S.C. §2703(d)* 2011: 127) of all people connected to the WikiLeaks Twitter account. US citizen Jacob Appelbaum, Dutch national Rop Gonggrijp, and Icelandic Member of Parliament Birgitta Jónsdóttir challenged the legality of this subpoena and its extension to 637,000 followers of WikiLeaks on Twitter. Appelbaum, Gonggrijp, and Jónsdóttir had provided various forms of assistance to Assange, which facilitated the global publication of classified military information leaked by Private Manning. The scale and extraterritorial reach of the Twitter subpoena is legally valid under the US Stored Communications Act (SCA) because Twitter is a US-based corporation that facilitates transnational communication amongst its subscribers.

The streamlined warrant procedures under the US SCA attempt to minimize ‘investigative delays caused by the cross-jurisdictional nature of the internet’ (*In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 2014: 473). This important element of the ‘digitally efficient investigative state’ (Rushin 2013) eliminates the cumbersome process of cross-jurisdictional requests to access online communications within the US, which required

(a)n investigator ... located in Boston who is investigating a suspected terrorist in that city ... [to] coordinate with agents, prosecutors and judges in the district of California where the ISP is located to obtain the warrant to search.

(*In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 2014: 473)

The ruling indicates the SCA reflects the ‘peculiar nature of electronic data’, which is more susceptible than ‘traditional physical evidence’ to being ‘overwritten, transferred, or expunged with little to no human effort’ (*In Re Application for the USA for an Order Pursuant to 18 U.S.C. §2703(d)* 2011: 143). As with any preliminary investigative hypothesis involving physical or digital evidence, the court indicated some information obtained via the subpoena ‘will not be material’ (*In Re Application for the USA for an Order Pursuant to 18 U.S.C. §2703(d)* 2011: 144). Nevertheless, the rights of those affected are ‘doubly protected’ under the SCA requirement for judicial authorization of the initial subpoena and further independent scrutiny of these surveillance processes in grand jury proceedings. Although personal information disclosed to third parties is not classified as a Fourth Amendment ‘search’ (*In Re Application for the USA for an Order Pursuant to 18 U.S.C. §2703(d)* 2011: 133-139), the decision by Appelbaum, Gonggrijp, and Jónsdóttir to legally challenge the subpoena ‘voluntarily disclosed that there may be some association’ between their activities and WikiLeaks (*In Re Application for the USA for an Order Pursuant to 18 U.S.C. §2703(d)* 2011: 146). Therefore, the very decision to challenge the legality of the subpoena negated any ‘chilling effect’ on their collective rights to free speech or association. In addition, by accepting the Terms of Service agreement as a condition of accessing Twitter, all users agree that their communications are ‘governed by the laws of the State of California’ (Twitter 2015: 12B), regardless of their physical location or nationality. Hence, there is no extraterritorial component to the SCA subpoena,

because all online communications are subject to the ‘law of the place’ where Twitter conducts its business.

Similar reasoning endorsed a SCA warrant ordering Microsoft to provide US law enforcement authorities with the contents of emails in a US citizen’s account, even though the server containing the data was in Ireland (*In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 2014). The account in question was one of many rerouted through an offshore server to increase data traffic speeds for US subscribers. Microsoft argued the warrant would only be valid if accompanied by a mutual legal assistance request requiring Irish authorities to obtain and transfer the data to US law enforcement agents (Microsoft 2014: 12). As with extradition, the burden of deciding whether and how any ‘documents, records and articles of evidence’ from foreign ‘searches and seizures’ are obtained and transferred is placed on the nation where the suspect or information is located (Department of State 2001: Art 1(2)). This procedure reflects the centrality of territorial sovereignty in limiting the extraterritorial investigative power of any nation through a process of reciprocal requests. However, the Microsoft ruling stressed mutual legal assistance provides unnecessary barriers to US law enforcers ‘where no treaty is in place’ (*In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 2014: 475). Further, there is also a risk that evidence could be declared inadmissible in criminal proceedings if law enforcement agencies in the state acting on a request violate their own laws governing the search, seizure and transfer of evidence (Palmer and Warren 2013).

These problems are sidestepped in the Microsoft ruling, which found a US company is obliged to provide any data under its control that is subject to a SCA warrant regardless of its geographic location. The court emphasized the Microsoft warrant did not contravene the presumption against extraterritorial investigative activity that requires a simultaneous mutual assistance request, because

an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; [and] it does not require even the physical presence of service provider employees at the location where data are stored.

(*In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 2014: 475)

Both of these cases stretch established principles of territorial sovereignty to facilitate prompt and efficient police access to digital information. Almost identical logic informs a series of Australian federal counterterrorism reforms enacted in 2015 that require ISPs to retain all client metadata for up to two years, which can be accessed by police without a warrant. Proponents of the reforms continually stressed the procedural burdens and time delays associated with obtaining warrants in serious ‘terrorism, drug trafficking, child exploitation and murder’ investigations (MacGibbon 2015), despite concerns that mass dataveillance is neither ‘necessary’ nor ‘proportionate’ to achieving ‘targeted’ law enforcement objectives (Australian Privacy Foundation 2015). Highly emotive cases where rapid warranted data access contributed to the prompt apprehension of predatory violent offenders (Milivojevic and McGovern 2014), or inadequate metadata retention periods compromised intervention in ‘a potential child rape case’ (Wroe 2015), provided the main justifications for streamlined data access to pre-empt serious crime and improve efficiency in future criminal investigations. However, the emphasis on serious violent crime underscores a deeper series of concerns surrounding the more efficient detection, prosecution and use of civil claims for online intellectual property violations through Australian ISPs (Palmer and Warren 2013: 106-108). A salient reminder of the centrality of these reforms to domestic and extraterritorial copyright enforcement involves a significant ruling by the Federal Court of Australia in April 2015, which ordered several ISPs to provide US copyright holders with the identification details of 4,726 individuals who allegedly accessed

the film *Dallas Buyers Club* through the BitTorrent peer-to-peer file sharing network (*Dallas Buyers Club LLC et al. v. iinet et al.* 2015).

Criminal Law and Mass Extraterritorial Surveillance

US laws validate the mass surveillance of non-US citizens who use online facilities operated by US companies. The legal classification of electronic data as property *controlled* by ISPs and corporations such as Twitter and Microsoft overlooks the end-user's conception of its personal or personally identifiable status. By not classifying this form of law enforcement surveillance as an extraterritorial incursion into foreign sovereign territory, these interpretations of the scope of criminal law enable US law enforcement officials to compile detailed mosaics of the online and real-world activities of many non-US citizens. The Terms of Service agreement is evidence of the end-user's voluntary acceptance of US criminal jurisdiction, reinforced by a logic that replicates the anomalous private and public spatial analogies that limit police investigative and surveillance powers in domestic criminal law. While these processes are deemed to comply with US constitutional due process and free speech requirements (see Rushin 2013), it remains conjectural whether these protections extend to 'the people' who are not US citizens.

Transnational law enforcement surveillance is framed by the mono-analogical concept of corporate 'control'. This casts an important new dimension into the scale of US mass dataveillance post-Assange and Snowden. As the structural constraints of territoriality that confine the jurisdictional scope of law enforcement surveillance are breaking down, classifying offshore data as extraterritorial surveillance would undermine the very purpose of the US SCA. The same analogic process that declares any information conveyed to a third party loses its confidential status and can be readily accessed without a warrant (Kerr 2015), classifies extraterritorial police surveillance that impinges on another nation's sovereignty as legally acceptable under US law, because that information is owned and controlled by US corporations. Similarly, the burdensome warrant procedure unnecessarily impedes the ability of Australian police to efficiently investigate or prevent serious violent crime or persistent domestic and offshore copyright violations. However, these interpretations also redefine the meaning of due process to promote selective extraterritorial crime control imperatives because US corporations facilitate, and therefore control, most global digital communication platforms. Until these contradictions are reconciled through agreed transnational governance processes, criminal law and surveillance will remain indistinguishable in promoting contradictory, self-legitimizing and potentially unfair sovereign criminal justice objectives. Further analysis of these emerging contradictions is essential to understanding the shifting relationship between criminal law, sovereignty and surveillance.

References

- Australian Privacy Foundation. 2015. *Submission to the Parliamentary Joint Committee on Intelligence and Security: Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. 19 Jan: at http://www.apf.gov.au/parliamentary_business/committees/joint/intelligence_and_security/national_security_amendment_bill_2014/submissions.
- Brenner, S.W. and J.J. Schwerha. 2002. Transnational Evidence Gathering and Local Prosecution of International Cybercrime. *The John Marshall Journal of Computer and Information Law* 20(3): 347-395.
- Cohen, J. E. 2015. Studying Law Studying Surveillance. *Surveillance & Society* 13(1): 91-101.
- Cornwall Lewis, G. 1859. *Foreign Jurisdiction and the Extradition of Criminals*. London UK: John W. Parker and Sons.
- Dallas Buyers Club LLC and Voltage Pictures LLC v. iinet Limited, Internode Pty Ltd, Amnet Broadband Pty Ltd, Dodo Services Pty Ltd, Adam Internet Pty Ltd and Widebrand Networks Pty Ltd*. 2015. FCA 317.
- Department of State. 2001. *Mutual Legal Assistance Treaty Between The United States of America and Ireland*. Washington, DC: Department of State. Available at: <http://www.state.gov/documents/organization/129536.pdf>.
- Dubber, M.D. 2006. Comparative Criminal Law. In: *The Oxford Handbook of Comparative Law*, eds M. Reimann and R. Zimmermann, 1287-1325. Oxford: Oxford University Press.
- Hardy, K. and G. Williams. 2014. Terrorist, Traitor, or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information. *University of New South Wales Law Journal* 37(2): 784-819.
- In Re Application for the USA for an Order Pursuant to 18 U.S.C. § 2703(d)*. 2011. 830 F. Supp. 2d 114.

- In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*. 2014. 15 F. Supp. 3d 466.
- Lyon, D. 2014. Surveillance, Snowden, and Big Data: Capacities, Consequences and Critique. *Big Data and Society* 1(2): 1-13. Available at: <http://bds.sagepub.com/content/1/2/2053951714541861.full.pdf+html>.
- Kerr, O. 2012. The Mosaic Theory of the Fourth Amendment. *Michigan Law Review* 111(3): 311-354.
- Kerr, O. 2015. The Fourth Amendment and the Global Internet. *Stanford Law Review* 67(2): 285-329.
- MacGibbon, A. 2015. Access to Metadata is Vital for Crime Fighting: Says Internet Safety Advocate'. *The Age*, 1 Feb. Available at: <http://www.theage.com.au/it-pro/it-opinion/access-to-metadata-is-vital-for-crime-fighting-says-internet-safety-advocate-20150130-1322uw.html>.
- Microsoft. 2014. Microsoft Services Agreement. Available at: <http://windows.microsoft.com/en-au/windows/microsoft-services-agreement>.
- Milivojevic, S. and A. McGovern. 2014. The Death of Jill Meagher: Crime and Punishment on Social Media. *International Journal for Crime, Justice and Social Democracy* 3(3): 22-39.
- Milligan, L.M. 2011. Analogy Breakers: A Reality Check on Emerging Technologies. *Mississippi Law Journal* 80(4): 1319-1338.
- Palmer, D. and I. Warren. 2013. Global Policing and the Case of Kim Dotcom. *International Journal for Crime, Justice and Social Democracy* 2(3): 105-119.
- Pregelj v. Manison*. 1987. 51 NTR 1.
- Rothe, D. and K. Steinmetz. 2013. The Case of Bradley Manning: State Victimisation, Realpolitik and WikiLeaks. *Contemporary Justice Review* 12(2): 280-292.
- Rushin, S. 2013. The Legislative Response to Mass Police Surveillance. *Brooklyn Law Review* 79(1): 1-60.
- Slobogin, C. 2011. Comparative Empiricism and Police Investigative Practices. *North Carolina Journal of International Law and Commercial Regulation* 37(2): 321-348.
- Twitter. 2015. Terms of Service. Available at: <https://twitter.com/tos?lang=en>.
- Warren, I. 1995. An Air of Uncertainty: Private Security Regulation in Victoria. *Deakin Law Review* 2(2): 223-253.
- Warren, I. and D. Palmer. Forthcoming. *Global Criminology*. Pyrmont, NSW: Thomson Reuters.
- Wroe, D. 2015. Attorney-General George Brandis Says Metadata Limits Jeopardise Criminal Investigations. *Sydney Morning Herald*, 25 Jan. Available at: <http://www.smh.com.au/federal-politics/political-news/attorneygeneral-george-brandis-says-metadata-limits-jeopardise-criminal-investigations-20150124-12wjqr.html>.