Surveillance & Society

Article

Lawful Illegality: Authorizing Extraterritorial Police Surveillance

Ian Warren
Deakin University, Australia
ian.warren@deakin.edu.au

Monique Mann
Deakin University, Australia
monique.mann@deakin.edu.au

Adam Molnar
University of Waterloo, Canada
adam.molnar@uwaterloo.ca

Abstract

This paper examines Lisa Austin's (2015) concept of lawful illegality, which interrogates the legal foundations for potentially unlawful surveillance practices by United States (US) signals intelligence (SIGINT) agencies. Lawful illegality involves the technically lawful operation of surveillance powers that might be considered unlawful when examined through a rule of law framework. We argue lawful illegality is expanding into domestic policing through judicial decisions that sanction complex and technically sophisticated forms of remote online surveillance, such as the use of malware, remote hacking, or Network Investigative Techniques (NITs). Operation Pacifier targeted and dismantled the Playpen dark web site, which was used for distributing child exploitation material (CEM), and has generated many judicial rulings examining the legality of remote surveillance by the FBI. We have selected two contrasting cases that demonstrate how US domestic courts have employed distinct logics to determine the admissibility of evidence collected through the NIT deployed in Operation Pacifier. The first case, *United States v. Carlson* (2017 US Dist. LEXIS 67991), offers a critical view of the use of NITs by the FBI, with physical geography constraining the legality of this form of surveillance in US criminal procedure. The second case, *United States v. Gaver* (2017 US Dist. LEXIS 44757), authorizes the use of NITs because the need to control crime is believed to justify suspending the geographic limits on police surveillance to identify people involved in the creation and dissemination of CEM. We argue this crime control emphasis expands the reach of US police surveillance while undermining due process of law by removing the protective function of geography. We conclude by suggesting the permissive geographic scope of police surveillance reflected in *United States v. Gaver* (2017 US Dist. LEXIS 44757), and many other Playpen cases, erodes due process for all crime suspects, but is particularly acute for people located outside the US, and suggest a neutral transnational arbiter could help limit contentious forms of remote extraterritorial police surveillance.

Introduction

Developments in criminal procedural law are crucial to understanding how new remote surveillance technologies become legitimized in contemporary policing. While the Fourth Amendment to the United States (US) Constitution aims to curtail state intrusions into the private domain (Cuddihy 2009), many post-9/11 surveillance measures aimed at promoting national security lack oversight (Bauman et al. 2014). Using Lisa Austin's (2015) lawful illegality framework, we argue that the permissive legal regimes underpinning surveillance by Western signals intelligence (SIGINT) agencies are now filtering into routine forms of policing (Haggerty 2012) and evidence collection by sanctioning "government dragnets" (Slobogin 2010). Specifically, we demonstrate how Fourth Amendment and related procedural laws governing the admissibility of evidence are viewed in two cases examining the use of malware by US police investigating the distribution and viewing of child exploitation material (CEM) on the Playpen dark web site. Our argument extends Austin's (2015) lawful illegality framework, which was originally developed to explain how surveillance by SIGINT agencies becomes legitimized through law and demonstrates how these processes are also becoming normalized in criminal law enforcement.

Warren, Ian, Monique Mann, and Adam Molnar. 2020. Lawful Illegality: Authorizing Extraterritorial Police Surveillance. *Surveillance & Society* 18 (3): 357-369.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

and are commonly justified, or exploited, by rationalizing techniques used by US SIGINT agencies to foster their legitimacy.

Austin (2015) explains how "unilateralism" and "secrecy" shape the views held by intelligence agencies about the lawfulness of their surveillance activities. These processes also serve to restrict knowledge about the contexts or scale of surveillance, which stifles external criticism. The closed organizational structures of most SIGINT agencies fortify their interpretations of the legality of, and necessity for, contentious surveillance tactics that are "routinely pushed as far as possible in the government's favor," while "actively sever[ing]" their impacts on due process (Austin 2015: 109–10; see also Packer 1968; Roach 1999). These self-validating interpretations test laws that are already structurally biased against public accountability. In other words, rather than clarifying ambiguities about the permissible scope of surveillance through public debate, SIGINT agencies adopt deliberate strategies that promote self-serving legal interpretations to justify their conduct and, at the same time, influence legislators and the judiciary to adopt similar views.

The second aspect of Austin's framework examines the "legal complexity" of SIGINT activities across different national and international institutions. Undue complexity leads to legislative reforms that erode independent oversight and weaken public accountability (Austin 2015: 110). This is done by stifling access to information about, and criticism of, surveillance "systems and methods" (Austin 2015: 113–14). SIGINT agencies insist surveillance is necessary to detect or prevent serious crimes. When combined, legal and technical complexity force judges to accept how covert operations are conducted on the advice of surveillance experts. This pattern is also demonstrated by McClain (2019: 253–54), who indicates judges and juries are unlikely to be equipped to properly understand or evaluate the technical complexity of expert evidence. Thus, both SIGINT and police agencies may exploit such legal and technical complexity to advance what is possible from an operational standpoint and garner the acceptance of these surveillance tactics by judges, the law, politicians, and the broader public.

Third, and importantly for our discussion, online SIGINT activities reflect "the technical imperatives of the nature of information" that transcend geographic borders (Austin 2015: 114; see also Daskal 2015, 2018; Svantesson 2017). This can significantly reorder the jurisdictional reach of governmental conduct. For Austin (2015), the current global "legal infrastructure" enables US SIGINT authorities to exploit self-validated motives for online surveillance in ways that are impervious to opposing legal or social perspectives (Mann and Warren 2018). An ensuing jurisdictional paradox emerges in "a global communications network where increasingly borders do not matter" when, in fact, borders are central in determining the limits of any state's authority to police and govern (Goldsmith and Wu 2006). In reconciling this paradox, it is important that legislators and judges ensure individuals have sufficient grounds to challenge contentious or coercive forms of police surveillance (Austin 2015: 118). Legal geography can play a pivotal role in limiting contentious extraterritorial police surveillance practices.

Legal Geography

Increasingly, the sovereign authority of much online surveillance and related criminal investigations is established by, and to serve, US interests (Bauman et al. 2014; Mann and Warren 2018; Mann, Warren, and Kennedy 2018). This is salient in transnational criminal investigations where conventional jurisdictional requirements do not necessarily match the enhanced surveillance capabilities of domestic agencies. Increasingly, criminal intelligence and evidence can be obtained remotely without the knowledge of relevant authorities in other jurisdictions (Warren 2015) or can be validated by exceptions to domestic legal constraints on police conduct. US precedent shows how exceptions to the Fourth Amendment have evolved to accommodate new domestic legal geographies that are adjusted to accommodate technologies that enhance social mobility. For example, during the prohibition era, the warrant requirement was considered to undermine police attempts to search motor vehicles suspected of transporting alcohol "because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought" (*Carroll v. United States*, 1925 267 US 132: 153; see also Grant 1941: 361). This led to judges developing the "reasonable suspicion" exception to the Fourth Amendment, which enhanced police discretion to conduct

on-the-spot vehicle searches (Grant 1941). However, this modification generated new dilemmas associated with discretionary decisions to deploy surveillance practices that reshaped the scope of reasonable suspicion (Slobogin 2010; Joh 2013). Similar problems informed US Postal Service stings that sought to identify recipients of printed CEM mailed from Europe during the 1980s (United States Department of Justice 1986: 653–655, 671–78; Hickson 1988; *Jacobson v. United States*, 1992 503 US 540; Chin 2012). Further, the offshore aerial surveillance of surface and semi-submerged vessels carrying illicit drugs on the open seas either to or via the US informed judicial modification of evidentiary rules to support the prosecution of foreign nationals (Warren and Palmer 2015). Remote GPS tracking technologies have created similar challenges (Dowdell 2005; Hutchins 2007), although their use is now considered to be a Fourth Amendment search that requires a warrant (*United States v. Jones*, 2012 565 US 400; *Grady v. North Carolina*, 2015 135 S. Ct. 1368).

US literature examining the legality of NITs mirrors these concerns, but with a more complex interplay of intra- and extraterritorial legal factors (Raustiala 2009). For example, US law allows evidence to be admitted from warrantless offshore surveillance *and* enforcement activities (see Austin 2015: 119; Warren 2015; Ghappour 2017; Russell 2017). The absence of Fourth Amendment restrictions to SIGINT and police surveillance outside of US territory seemingly enables more efficient criminal enforcement and transnational cooperation. Kerr and Murphy (2017: 65) outline several examples of US prosecutions that were only possible after foreign law enforcement agencies used remote hacking tools. These offshore activities are authorized by the selective use of domestic laws and enforcement protocols by US agencies that favor the use of new surveillance technologies while exploiting gaps in the structure of transnational criminal justice cooperation, which fails to place limits on information sharing (Nadelmann 1993; Bowling and Sheptycki 2015; Boister 2015; Warren and Palmer 2015). These processes are incremental, and can be opposed in judicial decisions that deny search warrants or determine that improperly obtained evidence is inadmissible in criminal trials.

Remote Surveillance before Operation Pacifier

In re Warrant to Search a Target Computer at Premises Unknown (2013 958 F. Supp. 2d 753) demonstrates an initial reluctance by US federal district courts to authorize NITs, given their ability to obtain evidence outside national geographic borders. This case involved an unsuccessful request by US police agents to deploy a NIT in an online fraud investigation linked to an internet protocol (IP) address in South East Asia (*In re Warrant to Search a Target Computer at Premises Unknown*, 2013 958 F. Supp. 2d 753: 758). The warrant sought authorization "to hack a computer suspected of criminal use" (*In re Warrant to Search a Target Computer at Premises Unknown*, 2013 958 F. Supp. 2d 753: 755) by remotely installing malware onto the target device. This would relay IP addresses, search engine terms, usernames, passwords, email contents, and device contacts to US authorities and would even exploit the device's camera and microphone to determine its *physical* location (*In re Warrant to Search a Target Computer at Premises Unknown*, 2013 958 F. Supp. 2d 753: 755–756). A US federal magistrate judge determined this form of surveillance unduly exceeded the sanctioned territorial limits on the US district court's jurisdiction, which would allow "FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing [federal] district" (*In re Warrant to Search a Target Computer at Premises Unknown*, 2013 958 F. Supp. 2d 753: 757).

Significantly, this ruling stressed that a valid US search warrant only authorizes the search of a "physical space with local habitation and a name" rather than "the airy nothing of cyberspace." Otherwise, there would be "no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district regardless of where it might initially be found" (*In re Warrant to Search a Target Computer at Premises Unknown*, 2013 958 F. Supp. 2d 753: 757). This reasoning is important because it explicitly constrains US police surveillance within geographic limits. In addition, by requiring judicial approval for its offshore NIT operation, the warrant enhances transparency, which, in turn, becomes a precondition for the evidence being viewed as admissible in a US criminal trial. This ruling, therefore, places limits on police jurisdiction that are grounded in physical territory. It demonstrates the

judicial willingness to limit police surveillance by recognizing the territoriality of data (Goldsmith and Wu 2006), which can be contrasted by viewing online activity through a logic that reflects the "precise blurring of boundaries, this limitless terrain of the possible where differences can inhibit the familiar, the homogeneous—that calls forth, that challenges, a security apparatus which, as Foucault (2007) tells us, does not function along the model of repression, but rather one of production, of allowance and license" (Bauman et al. 2014: 139).

However, since this initial ruling, the majority of US domestic cases examining the Playpen investigation appear willing to accept the blurred distinction between "surveillance for intelligence" and "surveillance for evidence" by suspending the geographic constraints on remote police surveillance (see American Civil Liberties Union, Electronic Frontiers Foundation, and National Association of Criminal Defense Lawyers 2017; hereafter cited in text as ACLU/EFF/NACDL). It is therefore important to examine how US courts have decided on the use of NITs for geographically limitless "surveillance for evidence" when determining its admissibility. Operation Pacifier forces US federal courts to reconsider the limiting requirements of the Fourth Amendment that are based on geography and territory in light of technologies that are commonly viewed as trans- or un-territorial (Daskal 2015).

Operation Pacifier and the Playpen Dark Web Site

The use of the dark web to disseminate CEM prompts arguments that new forms of extraterritorial surveillance are justifiable in domestic and transnational criminal investigations to render encrypted data visible (Kerr and Murphy 2017; Blakesley and Stigall 2004). As the dark web site Playpen could only be accessed through the Tor network, it employed encryption and a network of relays to conceal the locations and, by extension, identities of users (Mann and Warren 2018). Tor obfuscates the forensic reliability of data acquired through traffic analysis and the real-time interception of plain-text identifiers, as onion routing separates identification from location (Ghappour 2017: 1087 as cited in *United States v. Carlson*, 2017 US Dist. LEXIS 67991: 3). Relayed encryption is often used on the dark web for entirely legitimate purposes (Moore and Rid 2016; Gehl 2018; Lee 2018). However, the nefarious criminal applications of Tor provide seemingly uncontestable moral justifications for exceptional police surveillance (Kerr and Murphy 2017).

The circumstances leading to Operation Pacifier are central to understanding its status as a form of lawful illegality. In December 2014, an unspecified foreign law enforcement agency notified the FBI that a fixed geographic location for the Playpen servers could be determined from a leak of the administrator's IP address, which can occur when accessing public Wi-Fi networks (Mann and Warren 2018). On January 29, 2015, the FBI executed a search warrant at a residence in Naples, Florida, with a subsequent warrant leading to the apprehension of site administrator Steven W. Chase. The FBI then seized the *Playpen* server and relocated it to its facility in Newington, Virginia (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 5–7).

The NIT warrant was then sought by the FBI from a federal district magistrate under Rule 41 of the US Federal Rules of Criminal Procedure. This allowed the FBI to operate Playpen as a honeypot for up to thirty days from the Eastern District of Virginia and in five neighboring federal districts. Any device logging into Playpen would be infected with malware that relayed details about the user's login and password, IP address, and operating system to the FBI. This enabled the FBI to identify up to one million logins over a two-week period, involving around 158,000 visitors, or 1,500 visitors per day, who accessed "chat rooms, private messaging services and thousands of images of child pornography" (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 2). At least twenty-two thousand images of CEM were available for downloading, sharing, and viewing, which gathered information about eight thousand computers and users from internet service providers located throughout the US and 120 additional countries (Cox 2016). Domestically, the operation identified twenty-six child victims and led to charges against 137 US-based producers and consumers of CEM (*United States v. Kim*, 2017 US Dist. LEXIS 11770: 10–11). These cases are likely to take several years to work their way through the US federal courts.

At the time of writing, most Playpen cases remain undecided or favor classifying the NIT as a valid Fourth Amendment search, even though its geographic scope went beyond the Eastern District of Virginia and its five neighboring federal districts (see ACLU/EFF/NACDL 2017). While the NIT was deployed under the geographically flawed warrant, this is not considered sufficiently "outrageous" to justify declaring evidence from a computer located outside of these authorized geographic areas to be inadmissible (see Bambauer and Massaro 2015; ACLU/EFF/NACDL 2017).

Our argument is based on two cases with conflicting outcomes that exemplify (Flyvbjerg 2006) the contradictory judicial perspectives regarding the legality of Operation Pacifier and demonstrate the variations between crime control and due process views of criminal procedure (Packer 1968; Roach 1999). These contrasting cases reveal how US judges determine the admissibility of evidence obtained through the NIT deployed in Operation Pacifier and, in turn, how distinct forms of reasoning on the same issue reflect key elements of lawful illegality (Austin 2015). *United States v. Carlson* (2017 US Dist. LEXIS 67991) is considered one of the more serious Playpen cases, involving four counts of distributing, one count of receiving, and one count of possessing CEM under ß2251 and ß2252 of the US Code. We review the initial decision handed down on March 23, 2017, which used geography to circumscribe police surveillance through a strong due process logic, but was later overturned on appeal on August 7, 2017 (*United States v. Carlson*, 2017 US Dist. LEXIS 124452). Four days after the first ruling in *Carlson* (2017 US Dist. LEXIS 67991), *United States v. Gaver* (2017 US Dist. LEXIS 4475: 4) adopted a crime control logic that supported the legality of the NIT for "[s]everal charges of possession[,]… knowingly accessing with intent to view," and receiving "child pornography." The opposing perspectives are striking, as they consciously deal with the same surveillance issues through distinct legal perspectives, given the ruling in *Carlson* was expressly resisted in *Gaver*. These contested logics reveal how key elements of lawful illegality reshape the notion of due process in SIGINT and police investigations that utilize remote hacking and surveillance technologies to promote crime control objectives.

Geography and Due Process: *United States v. Carlson*

A report by the ACLU/EFF/NACDL (2017) identifies *United States v. Carlson* (2017 US Dist. LEXIS 67991) as one of five cases from the forty-seven decided between January 2016 and March 2017 that favored excluding all evidence. This is because the warrant failed to identify the specific place to be searched, which was considered a constitutionally significant violation of the geographic restrictions of Rule 41(b) of the Federal Rules of Criminal Procedure (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 14–15). Therefore, the first *Carlson* ruling mirrors the outcome of *In re Warrant to Search a Target Computer at Premises Unknown* (2013 958 F. Supp. 2d 753) by suggesting that, rather than acting in good faith on the federal magistrate judge's jurisdictional error, the FBI intentionally instigated an excessive and unlawful domestic surveillance program that prejudiced the defendant's criminal trial (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 23).

Carlson (2017 US Dist. LEXIS 67991) found that all evidence from the NIT warrant, including derivative physical evidence, must be excluded. This was because the FBI's warrant application prompted a substantive error by "the Magistrate Judge in the Eastern District of Virginia [who] lacked territorial jurisdiction to issue the NIT warrant" (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 22). This made the warrant void *ab initio*, which means it is to be considered "as if… [it] never existed" or "akin to no warrant at all" (*United States v. Croghan*, 2016 US Dist. LEXIS 127479; *United States v. Levin*, 2016 US Dist. LEXIS 52907: 37 as cited by *United States v. Carlson*, 2017 US Dist. LEXIS 67991: 22–23). The expansive geographic scope and invasive character of the NIT were central to this decision, as was the court's view that experienced FBI agents knew they were engaging in a global "fishing" exercise when making the original warrant application (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 15). Therefore, after the search warrant was issued, "neither the Government nor the issuing Magistrate Judge had any idea which computers, out of all the computers on the planet, might be infected by the Government's invasive malware' (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 8). The ruling continued by questioning the legality of this form of remote surveillance:

> Stated differently, the Government claims legal authority from this single warrant, issued in the Eastern District of Virginia, to hack thousands of computers in 120 countries and to install malicious software for the purpose of investigating and searching the private property of uncounted individuals whose identities and crimes were unknown to the Government before launching this massive worldwide search. (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 10)

This geographic emphasis has two components. The first is the *lack of particularity* in the warrant, which failed to identify the physical location of the search with sufficient precision. Rather, the warrant described "a process by which the place to be searched can in the future be ascertained by a Government controlled 'computer server'" for "the TARGET WEBSITE identified by its URL upf45jv3bziuctml.onion," but was otherwise "geographically silent" and only able to "identify which computers will be searched… [after] the search is actually completed" (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 34–35, 40). The second component is the possibility that the NIT could be viewed as a tracking device under Rule 41(b)(4), which was installed in the Eastern District of Virginia, travelled the world, then relayed relevant information back to the FBI servers about target computers in various fixed locations that visited the Playpen honeypot (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 17–18). Referring to two previous Playpen cases (*United States v. Torres*, 2016 US Dist. LEXIS 122086 and *United States v. Henderson*, 2016 US Dist. LEXIS 118608), the court rejected this argument "because the NIT was installed on Carlson's activating computer in Minnesota, not in the Eastern District of Virginia… [and] *the FBI 'itself did not believe the NIT was a tracking device*'" (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 18–19, emphasis added). This reveals how courts can defer to FBI expertise. Supporting decisions in other relevant cases, *United States v. Carlson* (2017 US Dist. LEXIS 124452: 21) also affirmed that the "computer information that the NIT targeted was at all relevant times located beyond the boundaries of the Eastern District of Virginia." As such:

> neither the search of Carlson's activating computer pursuant to the NIT warrant nor the searches pursuant to the two warrants issued in the District of Minnesota would have occurred without the violation of Rule 41(b)... [and] the FBI would not have obtained the identifying information from Carlson's activating computer or Carlson's IP addresses, would not have been able to link that IP addresses to Carlson's residence through subsequent investigation and administrative subpoenas, and would not have had sufficient evidence to support a probable cause showing to obtain the warrants issued in the District of Minnesota. (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 24–25)

Unlike most prior rulings that found "the issuing Magistrate Judge recklessly disregarded the limits of her own authority," *Carlson* considered the FBI agent acted in "reckless disregard for proper procedure" when making the NIT warrant application (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 27–28). This was considered a substantive violation of Rule 41 that "unconstitutionally expanded the scope of the NIT warrant by searching Carlson's computer located outside the Eastern District of Virginia," and was "of [such] constitutional magnitude" to justify excluding all evidence obtained through the NIT (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 41). This included all derivative evidence, such as data taken from a physical search of Carlson's computer and any verbal admissions of guilt he later made to arresting officers (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 40, 42, 45–50).

This view concluded that the warrant emanated from a defect in police procedure. The court determined that the FBI substantively and flagrantly misled the federal magistrate judge, and that it could not be accepted that its agents had acted in good faith to justify admitting the evidence. Rather, the court believed police played a tactical game with the potential to disadvantage any person who entered the Playpen site during Operation Pacifier, and characterized the FBI's misconduct in scathing terms worth documenting in full:

> The purpose and flagrancy of the FBI's misconduct in attempting to obtain the NIT warrant and deploying the NIT malware is truly staggering. In order to identify Playpen users, the FBI operated a copied version of a dark web, child pornography website for two weeks. During that period, countless images and video content depicting child pornography were globally downloaded and distributed via the Playpen. In essence, the FBI facilitated the victimization of minor children and furthered the commission of a more serious crime - the distribution of child pornography - to primarily identify offenders committing less serious crimes-viewing and receipt of child pornography. Moreover, although the January 15, 2015, warrant… judicially authorized the FBI to seize the Playpen's domain URL, that warrant did not authorize the FBI to then independently operate the website and house and disseminate the very content it now accuses hundreds of defendants of receiving. (*United States v. Carlson*, 2017 US Dist. LEXIS 67991: 53–54)

This reasoning considers it unfair to admit any evidence obtained from these procedural violations, which intentionally misled the federal magistrate judge into exceeding the permitted geographic scope for issuing a warrant under Rule 41(b). In other words, the federal magistrate judge was misled by the FBI into accepting that the NIT warrant was necessary to identify users of Playpen, despite its dubious geographic scope and implications for due process.

Policing and Technological Deference: *United States v. Gaver*

United States v. Gaver (2017 US Dist. LEXIS 44757: 31n6) also examined the integrity of police conduct, but did not incorporate the report and recommendation adopted in the first *Carlson* (2017 US Dist. LEXIS 67991) ruling to prevent the admission of evidence from the NIT. Gaver's ancillary legal claims, which were rejected, turned on the altered appearance of the Playpen site after it was seized by the FBI and on the extent to which the NIT source code should be disclosed for forensic examination (see Owsley 2017). These issues hinged on attributing the unlawful character of the extraterritorial warrant to the federal magistrate judge, rather than FBI misconduct. As per *Carlson* (2017 US Dist. LEXIS 67991), the latter approach would have suppressed all evidence collected from the NIT, including derivative evidence. Gaver's main argument was that, without the defective NIT warrant, "the government would not have discovered Gaver's IP address and would not have obtained the warrant to search his apartment." Therefore, prosecutors should not benefit from the "fruits of the poisonous [NIT] tree" (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 5, 21).

Gaver challenged statements provided by the FBI to the federal magistrate judge indicating that "the property to be searched is located in the Eastern District of Virginia" (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 19). This is where the "TARGET WEBSITE" was physically relocated by the FBI for the duration of the NIT warrant. However, the FBI affidavit specified data would be collected from "activating computers" located outside this district (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 34–35, 20), as "the NIT will cause the activating computer, 'wherever located,' to transmit certain information to a government computer to help identify the location of the computer and its user."

This reasoning has been embraced by most US courts that have found the federal magistrate judge lacked authority to issue the NIT warrant outside of the Eastern District of Virginia (see *United States v. Gaver*, 2017 US Dist. LEXIS 44757: 22; ACLU/EFF/NACDL 2017). As with the first *Carlson* case, the NIT was not classifiable as a tracking device (cf. *United States v. Matish*, 2016 193 F. Supp 3d 585; *United States v. Darby*, 2016 190 F. Supp 3d 520; *United States v. Jean*, 2016 US Dist. LEXIS 123869) because the malware was not installed in the Eastern District of Virginia and gathered information from the fixed positions of recipient computers located elsewhere. However, even though the federal magistrate judge was considered to have lacked jurisdiction to issue the warrant, the evidence was admissible, as there was no proof that its suppression would deter future FBI misconduct or excessive police surveillance. In other words, it was determined that FBI operatives showed no conscious or reckless intention to mislead the federal magistrate judge when applying for the warrant and had no intention to violate the geographic restriction in Rule 41(b).

This view places responsibility for the violation solely on the federal magistrate judge (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 30). In line with other rulings in the sixth US federal circuit, the benefits of enhancing the detection of CEM readily superseded any perceived legal or social costs of remote NIT surveillance, as:

> …individuals involved in the dark underworld of child pornography go to great lengths to avoid detection. But for tools like the NIT, law enforcement officers may never be able to identify these individuals and bring them to justice… the costs to society of suppressing the evidence are significantly outweighed by the benefit of deterrence…[and] the good faith exception to the exclusionary rule applies in this case. (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 33).

Gaver was given access to the payload instructions from the NIT that was linked to his computer and a list of all information collected from the remote search as well as the two-way network data stream, the code generating unique identifiers for each computer logging into Playpen during Operation Pacifier, and a list of his online activities during the operation (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 7). However, the court was unwilling to compel the FBI to release details about the zero-day exploit that compromised Tor's encryption or the server that stored information collected from the NIT. This was in line with decisions in other US courts (*United States v. Matish*, 2016 193 F. Supp 3d 585; *United States v. Darby*, 2016 190 F. Supp 3d 520; *United States v. Jean*, 2016 US Dist. LEXIS 123869; *United States v. Tippens*, 2016 US Dist. LEXIS 184174; *United States v. McLamb*, 2016 US Dist. LEXIS 163990, *United States v. McLamb*, 2017 US Dist. LEXIS 7766), which found this material was subject to qualified law enforcement privilege and involved an "impermissible 'fishing expedition'" that would "severely compromise future investigations" or could enable technological countermeasures to be developed that subvert the surveillance capabilities of the NIT and ultimately justified "the government's need to keep it secret" (*United States v. Gaver*, 2017 US Dist. LEXIS 44757: 11).

Gaver (2017 US Dist. LEXIS 44757: 35) favored the view that the NIT warrant outlined the "particular places and things to be searched, i.e., the computers of anyone who logged onto the PlayPen website," with sufficient precision by ensuring that only the criminal activity of "each individual who logged onto" the honeypot would be detected. Hence, the warrant was not considered overbroad or general, but, rather, was a legacy of the anomalous geographic requirements of Rule 41(b) at the time of Operation Pacifier. This view emphasizes that the locus of responsibility for granting the geographically flawed warrant rested with the federal magistrate judge rather than FBI operatives who applied for the warrant, and ensured any evidence collected through this form of remote surveillance was admissible because the police acted in good faith when following the terms of the defective warrant.

Discussion

Our analysis extends Austin's (2015) lawful illegality framework into the realm of criminal investigations. We have sought to reveal the legal complexity underpinning online investigations and the challenges facing domestic US courts when determining the admissibility of evidence collected through remote NIT surveillance. We contend that the authorized territorial scope of police surveillance is expanding through judicial decisions that validate remote surveillance, which crisscrosses national and international jurisdictions. These developments are recognized in surveillance literature examining SIGINT (Bauman et al. 2014; Austin 2015), yet are overlooked in the context of online surveillance by police agencies. Operation Pacifier is an important example demonstrating how US judicial decisions grapple with otherwise hidden forms of warrantless intelligence collection on the surface or dark webs, which are increasingly brought to light in criminal trials (see Slobogin 2010; Mützel 2019).

The conflicting logics in *Carlson* (2017 US Dist. LEXIS 67991) and *Gaver* (2017 US Dist. LEXIS 44757) indicate how discrete components of lawful illegality underpin the strategies behind emerging police surveillance programs for evidentiary purposes. Lawful illegality helps to explain jurisdictional arguments

that inform the laws governing surveillance and police procedure. While there are contradictory outcomes in our case exemplars, they also bear similarities.

Austin (2015) argues that technological imperatives redraw the basic logic of jurisdictional aspects of surveillance by SIGINT agencies. We have shown that US courts formalize lawful illegality in ways that render the distinctions between policing and intelligence meaningful, even if they are also blurred. This is because police need to operate with more transparency than the intelligence community, but this heightened transparency does not necessarily translate into the rejection of invasive police surveillance by US courts. In criminal investigations since *In re Warrant to Search a Target Computer at Premises Unknown* (2013 958 F. Supp. 2d 753), US judges have struggled to reconcile the geographic constraints of jurisdiction with new surveillance technologies. This conundrum magnifies the legal complexity of determining the admissibility of criminal evidence, which places immense trust in the technical knowledge of police and other expert witnesses (McClain 2019). In line with Austin, such complexity can obfuscate basic principles of due process and procedural fairness.

Unlike SIGINT agencies, police agencies must obtain judicial authorization for search and seizure. In Austin's terms, they are not acting unilaterally, but are subject to judicial oversight. However, in *Gaver* (2017 US Dist. LEXIS 44757), judicial acceptance of the police's reasoning that justified the NIT warrant validated remote extraterritorial searches within the US. This is because FBI agents are believed to have acted in *good faith*. In contrast, the first *Carlson* (2017 US Dist. LEXIS 67991: 53) ruling emphasized that the "flagrancy of the FBI's misconduct in attempting to obtain the NIT warrant and deploying the NIT malware is truly staggering," and this was considered to have misled the federal magistrate judge into granting the warrant. The transition from SIGINT-style warrantless "surveillance for intelligence" to "surveillance for evidence" demonstrates courts have considerable latitude in the way admissibility is framed and decided. This movement from intelligence gathering to policing for the collection of admissible evidence implicates the need for clear rules governing the disclosure, scrutiny, and accuracy of the tactics authorized under a warrant, which can later be subject to cross-examination. By extension, these distinct classifications also determine the legality of the surveillance techniques adopted by police (Slobogin 2010; Friedman 2017).

Gaver (2017 US Dist. LEXIS 44757) reinforces the apparent "good faith" of the FBI's use of the NIT, while masking its attempt to pursue a favorable legal interpretation that substitutes targeted search and seizure requirements in a defined physical location with a geographically limitless "probable cause" justification. The centrality of geography is crucial, as the NIT can identify the physical location of any person who logs into the target website. Therefore, although the warrant was technically void, police were considered to have acted innocently, and in good faith, to justify an *ex post* ruling that the NIT was lawfully deployed. In contrast, in the first *Carlson* (2017 US Dist. LEXIS 67991) case, the FBI was considered to have known the NIT would readily transcend the geographic restrictions in Rule 41 at that time. This favored placing a clear legal bar on the scope of permissible surveillance, which suggests Operation Pacifier was an intentional attempt to flout the concept of good faith by subverting geographic limits on federal warrant jurisdiction (see also Gillum 2019).

Thus, the scope and limits of Fourth Amendment protections in the US are variable, and can be readily disturbed by the legal interpretations of experienced police agents seeking judicial authorization to use NITs. However, the second ruling in *Carlson* (2017 US Dist. LEXIS 124452) shows that such decisions can also fall readily in line with opinions that validate extraterritorial police surveillance. Experienced investigators have considerable power to assert that new surveillance techniques are necessary (Nadelmann 1993), to intentionally test the geographic boundaries that limit their categorization as *lawful*. We consider Operation Pacifier as a contemporary equivalent to the modification of the "reasonable suspicion" doctrine in motor vehicle cases from the 1920s that is recast through the "good faith" exception. While these attributes may not be *unilateral* in the sense that Austin (2015) noted in the permissive surveillance realms of SIGINT, they demonstrate judicial deference to police expertise serves to redraw the accepted boundaries of due process while amplifying the degree of legally permitted surveillance for criminal enforcement purposes.

These developments expand beyond the US to constitute a new form of global policing sanctioned by US legal and surveillance infrastructures (Warren and Palmer 2015; Bowling and Sheptycki 2015; Ghappour 2017). Operation Pacifier is another form of US "legal imperialism" (Mann and Warren 2018), involving the self-authorized extension of US extraterritorial police power outside its sovereign territory. By declaring evidence collected from outside of the five neighboring districts of the Eastern District of Virginia admissible, domestic courts have relaxed the jurisdictional constraints on FBI surveillance that are readily subverted by the NIT. When extended to extraterritorial police surveillance, such evidence is considered admissible because the Fourth Amendment search and seizure protections do not apply outside of the US. US courts are complicit in expanding the gaze of US federal police surveillance outside its territory (Warren and Palmer 2015), which draws on the same logic that legitimizes the interterritorial expansion of police surveillance on US soil.

On December 1, 2016, the US government petitioned to remove the geographic restriction under Rule 41(b). This means federal magistrate judges now have the authority to issue warrants anywhere in the US. This will not affect unresolved cases stemming from Operation Pacifier, but it is now entirely lawful for the FBI and other US police agencies to conduct NIT operations where technologies are employed to mask geolocation. This development was promptly followed by the enactment of the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), which enables US police agencies to compel US technology companies to provide access to data located extraterritorially to the US (United States Department of Justice 2019; Warren 2015). Taken together, these measures reinforce a pattern of self-authorized domestic and international police surveillance under US criminal procedural law. Therefore, the US can "unilaterally" surveil outside the US and then deem evidence admissible in criminal trials regardless of where the suspects are located.

Conclusion

This paper demonstrates the importance of examining the ways judicial decisions redraw the contours of domestic surveillance powers. The use of malware and other forms of remote surveillance implicate notable step-changes in the expansion of domestic police powers (Molnar, Parsons, and Zouave 2017) and the erosion of due process within a logic that confers priority on crime control (Packer 1968; Roach 1999). NITs are powerful surveillance techniques in the contemporary police armory that are granted legal legitimacy through the same processes that validate SIGINT procedures. Our analysis demonstrates how lawful illegality can help to explain how the logic of "surveillance for intelligence" permeates into policing by removing geographic constraints to collect evidence through remote surveillance, or government hacking, to be ruled as admissible in criminal trials. However, we demonstrate that the crime control logic supporting "surveillance as evidence" can equally be reconfigured to respect due process and the rule of law if courts are willing to recognize how geography can limit the scope and reach of police surveillance.

The view that NITs are justifiable prioritizes crime control over due process. Limits to expanding domestic police surveillance might now be lost with the suspension of geographic restrictions in the amendments to Rule 41. However, alternate approaches may be established to deal with the offshore implications of these processes, such as a neutral forum of *trans*national criminal law and procedure (Boister 2015). Limiting the surveillance reach of national law enforcement agencies through such arrangements may be the most viable means to consider given the appeal of remote surveillance technologies for crime control and the introduction of new US laws removing the need for judicial scrutiny to allow the prompt exchange of digital evidence with and from other nations (United States Department of Justice 2019). A neutral venue for openly scrutinising transnational police surveillance of a nation's citizens or residents, or the international harmonization of privacy and data protection laws, demand consideration as possible alternatives to demarcating authority through diluted territorial lines that assume geography is irrelevant to regulating transnational data flows. Even with a clear acknowledgment of the potential pitfalls of a coordinated approach to transnational data regulation, it is necessary for surveillance scholars to advance such inquiry to protect individuals from unconstrained transnational surveillance.

References

American Civil Liberties Union, Electronic Frontiers Foundation, and National Association of Criminal Defense Lawyers (ACLU/EFF/NACDL). 2017. *Challenging Government Hacking in Criminal Cases*. ACLU. https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf [accessed Apr 10, 2017].

Austin, Lisa M. 2015. Lawful Illegality: What Snowden Has Taught US about the Legal Infrastructure of the Surveillance State. In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 103–125. Ottawa, CA: University of Ottawa Press.

Bambauer, Jane R., and Toni M. Massaro. 2015. Outrageous and Irrational. *Minnesota Law Review* 100 (1): 281–354.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R.B.J. Walker. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8 (2): 121–124.

Blakesley, Christopher L., and Dan Stigall. 2004. Wings for Talons: The Case for the Extraterritorial Jurisdiction over Sexual Exploitation of Children Through Cyberspace. *Wayne Law Review* 50 (1): 109–159.

Boister, Neil. 2015. Further Reflections on the Concept of Transnational Criminal Law. *Transnational Legal Theory* 6 (1): 9–30.

Bowling, Benjamin and James Sheptycki. 2015. Global Policing and Transnational Rule with Law. *Transnational Legal Theory* 6 (1): 141-173.

Chin, Gabriel J. 2012. The Story of *Jacobson*: Catching Criminals or Creating Crime? In *Criminal Law Stories*, edited by Donna Coker and Robert Weisberg, 299–328. New York, NY: Foundation Press.

Cox, Joseph. 2016. Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile. *Motherboard*, January 23. https://motherboard.vice.com/en_us/article/qkj8q3/child-porn-sting-goes-global-fbi-hacked-computers-in-denmark-greece-chile?utm_source=vicefbuk&fbclid=IwAR0A_UUsm2oLM-SQCS-kIiX2_dLtRHv_zB4I8dZDInSWLyOtFoC5Sqx4e4g [accessed Mar 1, 2019].

Cuddihy, William J. 2009. *The Fourth Amendment: Origins and Original Meaning 602-1791*. Oxford, UK: Oxford University Press.

Daskal, Jennifer. 2015. The Un-Territoriality of Data. *The Yale Law Journal* 125 (2): 326–398.

———. 2018. Borders and Bits. *Vanderbilt Law Review* 71 (1): 179–240.

Dowdell, Eva Marie. 2005. You Are Here—Mapping the Boundaries of the Fourth Amendment with GPS Technology. *Rutgers Computer and Technology Law Journal* 32 (1): 109–139.

Flyvbjerg, Bent. 2006. Five Misunderstandings about Case Study Research. *Qualitative Inquiry* 12 (2): 219–245.

Friedman, Barry. 2017. *Unwarranted: Policing Without Permission*. New York, NY: Farram, Straus, and Giroux.

Gehl, Robert W. 2018. *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. Cambridge, MA: MIT Press.

Ghappour, Ahmed. 2017. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. *Stanford Law Review* 69 (4): 1075–1136.

Gillum, Jack. 2019. Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned. *ProPublica*, April 3. https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned?fbclid=IwAR39f9Z9Pk902blP9sQD-ej3GgUrcMlc1KICVGYCuYn5_8TLo3Z9GXzXBqo [accessed April 3, 2019].

Gless, Sabine. 2015. Bird's-Eye View and Worm's-Eye View: Toward a Defendant-Based Approach to Transnational Criminal Law. *Transnational Legal Theory* 6 (1): 117–140.

Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet: Illusions of a Borderless World*. Oxford, UK: Oxford University Press.

Grant, J.A.C. 1941. Circumventing the Fourth Amendment. *Southern California Law Review* 14 (4): 359–372.

Haggerty, Kevin D. 2012. Surveillance, Crime and the Police. In *The Routledge Handbook of Surveillance Studies*, edited by Kirsty Ball, Kevin D. Haggerty, and David Lyon, 235–250. London, UK: Routledge.

Hickson, Richard F. 1988. Privacy, Pornography and the Supreme Court. *The John Marshall Law Review* 21 (4): 755–776.

Hutchins, Renée McDonald. 2007. Tied up in *Knotts*? GPS Technology and the Fourth Amendment. *UCLA Law Review* 55 (2–3): 409–465.

Joh, Elizabeth E. 2013. Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion. *Arizona Law Review* 55 (4): 997–1029.

Kerr, Orin S., and Sean D. Murphy. 2017. Government Hacking to Light the Dark Web: Risks to International Relations and International Law? *Stanford Law Review* 70 (1): 58–69.

Lee, Murray. 2018. Crime and the Cyber Periphery: Criminological Theory Beyond Time and Space. In *The Palgrave Handbook of Criminology and the Global South*, edited by Kerry Carrington, Russell Hogg, John Scott, and Massimo Sozzo, 223–243. Cham, CH: Springer.

Mann, Monique, and Ian Warren. 2018. The Digital and Legal Divide: *Silk Road,* Transnational Online Policing and Southern Criminology. In *The Palgrave Handbook of Criminology and the Global South*, edited by Kerry Carrington, Russell Hogg, John Scott, and Massimo Sozzo, 245–260. Cham, CH: Springer.

Mann, Monique, Ian Warren, and Sally Kennedy. 2018. The Legal Geographies of Transnational Cyber-Prosecutions: Extradition, Human Rights and Forum Shifting. *Global Crime* 19 (2): 107–124.

Mayer, Jonathan. 2018. Government Hacking. *The Yale Law Journal* 127 (3): 570–662.

McClain, Noah. 2019. Caught Inside the Black Box: Criminalization, Opaque Technology and the New York Subway MetroCard. *The Information Society* 35 (5): 251–271.

Molnar, Adam, Christopher Parsons, and Erik Zouave. 2017. Computer Network Operations and "Rule-with-law" in Australia. *Internet Policy Review* 6 (1): 1–14.

Moore, Daniel, and Thomas Rid. 2016. Cryptopolitik and the Darknet. *Survival* 58 (1): 7–38.

Mützel, Daniel. 2019. Meet the Hacker Who Busts Child Pornographers on the Dark Net. Translated by Daniel Stächelin. *Vice*, February 27. https://www.vice.com/en_au/article/ywbmyb/meet-the-hacker-who-busts-child-pornographers-on-the-dark-net?fbclid=IwAR1mj3eRqCsJuJt0pKHAHuTGGSbYxfWC24qct0XRTaYt2UZHLxKc785iJJ0 [accessed April 3, 2019].
Nadelmann, Ethan. 1993. *Cops Across Borders: The Internationalization of US Criminal Law Enforcement*. University Park, PA: Pennsylvania State University Press.
Owsley, Brian L. 2017. Network Investigative Source Code and Due Process. *Digital Evidence and Electronic Signature Law Review* 14 (1): 39–46.
Packer, Herbert. 1968. *The Limits of the Criminal Sanction*. Stanford, CA: Stanford University Press.
Raustiala, Kal. 2009. *Does the Constitution Follow the Flag: The Evolution of Territoriality in American Law*. Oxford, UK: Oxford University Press.
Roach, Kent. 1999. Four Models of Criminal Process. *Journal of Criminal Law and Criminology* 89 (2): 671–716
Russell, Zoe. 2017. First They Came for the Child Pornographers: The FBI's International Search Warrant to Hack the Dark Web. *St Mary's Law Journal* 49 (1): 269–315.
Slobogin, Christopher. 2010. Government Dragnets. *Law and Contemporary Problems* 73 (3): 107–143.
Svantesson, Dan Jerker B. 2017. *Solving the Internet Jurisdiction Puzzle*. Oxford, UK: Oxford University Press.
United States Department of Justice. 1986. *Attorney General's Commission on Pornography: Final Report*. Washington: US Department of Justice.
United States Department of Justice. 2019. *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act.* Washington: US Department of Justice. https://www.justice.gov/opa/press-release/file/1153446/download [accessed February 12, 2020].
Walden, Ian, and Anne Flanagan. 2003. Honeypots: A Sticky Legal Landscape? *Rutgers Computer and Technology Law Journal* 29 (2): 317–370.
Warren, Ian. 2015. Surveillance, Criminal Law and Sovereignty. *Surveillance & Society* 13 (2): 300–305.
Warren, Ian, and Darren Palmer. 2015. *Global Criminology*. Pyrmont, NSW: Thomson Reuters.
Weidenhouse, Kurt C. 2017. Playpen, the NIT, and Rule 41(b): Electronic Searches for those Who Do Not Wish to Be Found. *Journal of Business and Technology Law* 13 (1): 143–69.

Statutes, Legislation, and Case Law

Carroll v. United States, 1925 267 US 132.
Grady v. North Carolina, 2015 135 S. Ct. 1368.
In re Warrant to Search a Target Computer at Premises Unknown, 2013 958 F. Supp. 2d 753.
Jacobson v. United States, 1992 503 US 540.
United States v. Carlson, 2017 US Dist. LEXIS 67991 (D. Minn Mar. 23).
United States v. Carlson, 2017 US Dist. LEXIS 124452 (D. Minn Aug. 7).
United States v. Croghan, 2016 US Dist. LEXIS 127479 (S.D. Iowa Sep. 29).
United States v. Darby, 2016 190 F. Supp 3d 520 (E.D. Va. Aug. 12).
United States v. Gaver, 2017 US Dist. LEXIS 44757, (S.D. Ohio Mar. 27).
United States v. Jean, 2016 US Dist. LEXIS 123869 (W.D. Ark. September 13).
United States v. Henderson, 2016 US Dist. LEXIS 118608 (W.D. Pa. Nov. 8)
United States v. Jones, 2012 565 US 400 (Jan. 23)
United States v. Kim, 2017 US Dist. LEXIS 11770 (E.D.N.Y. Jan. 17).
United States v. Levin, 2016 US Dist. LEXIS 52907, (D. Mass Apr. 20).
United States v. Matish, 2016 193 F. Supp 3d 585 (E.D. Va. Jun. 23).
United States v. McLamb, 2016 US Dist. LEXIS 163990 (E.D. Va. Nov. 28).
United States v. McLamb, 2017 US Dist. LEXIS 7766 (E.D. Va. Jan. 19).
United States v. Tippens, 2016 US Dist. LEXIS 184174 (W.D. Wash. Nov. 30).
United States v. Torres, 2016 US Dist. LEXIS 122086 (D.N.M. Jun 9).