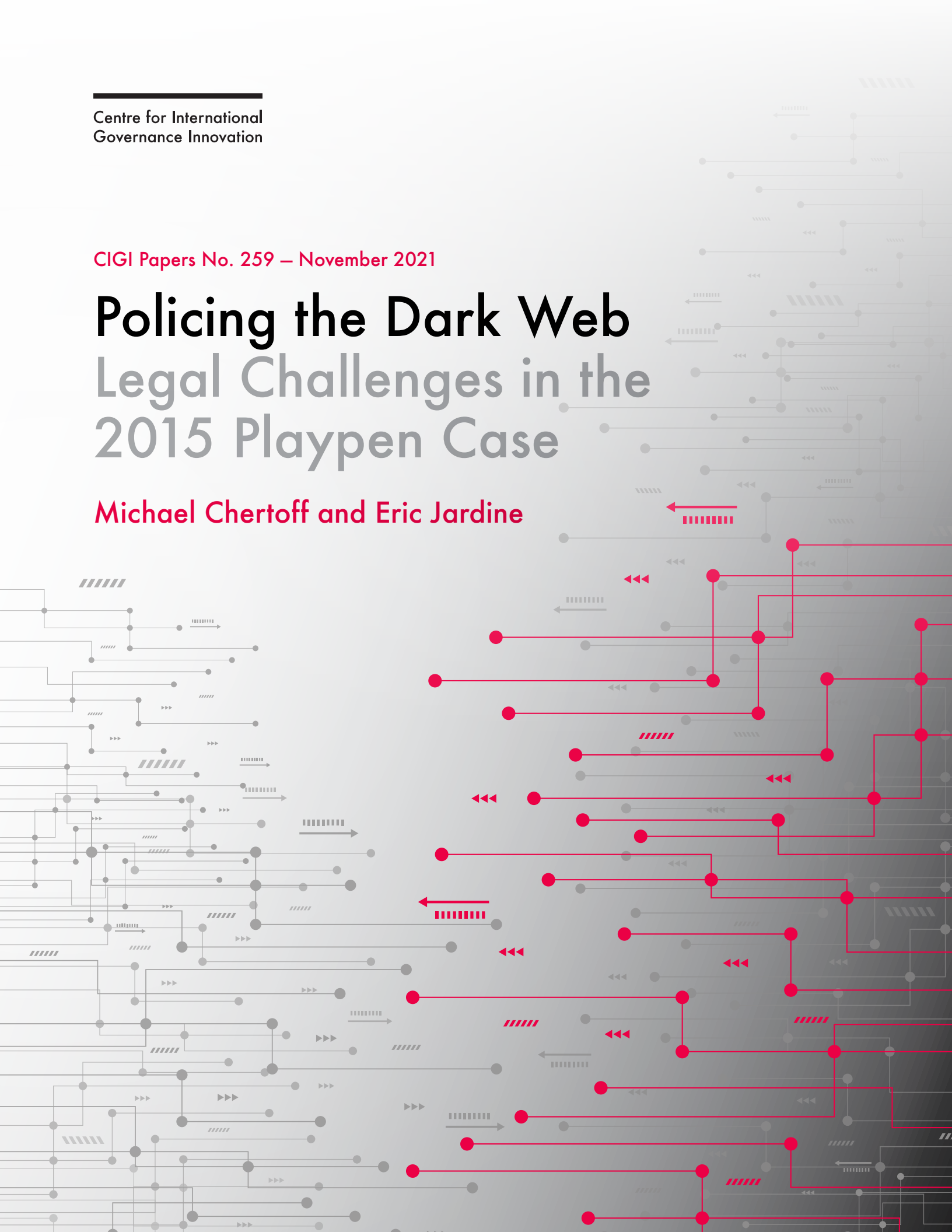
Centre for International
Governance Innovation

CIGI Papers No. 259 — November 2021

Policing the Dark Web
Legal Challenges in the 2015 Playpen Case

Michael Chertoff and Eric Jardine



Centre for International
Governance Innovation

CIGI Papers No. 259 — November 2021

Policing the Dark Web
Legal Challenges in the 2015 Playpen Case

Michael Chertoff and Eric Jardine

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Program Manager Aya Al Kabarity
Publications Editor Susan Bubak
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

Centre for International Governance Innovation and CIGI are registered trademarks.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Michael Chertoff is a distinguished fellow at CIGI, where he focuses on cybersecurity. Michael was also a commissioner with CIGI's Global Commission on Internet Governance.

Prior to joining CIGI, Michael served as secretary of the US Department of Homeland Security, where he led the government's efforts to protect the United States from a range of security threats, including cybersecurity and border threats.

Earlier, he served as a federal judge on the US Court of Appeals for the Third Circuit and as head of the US Department of Justice's Criminal Division.

Michael currently serves as the executive chairman and co-founder of the Chertoff Group, a global advisory firm that provides business strategy, risk management, and mergers and acquisition advisory services to clients seeking to secure and grow their enterprises.

He is a magna cum laude graduate of both Harvard College and Harvard Law School.

Eric Jardine is a CIGI fellow and an assistant professor of political science at Virginia Tech. Eric's research focuses on the uses and abuses of the dark web, measuring trends in cybersecurity, how people adapt to changing risk perceptions when using new security technologies, and the politics surrounding anonymity-granting technologies and encryption.

His work has been published in a number of peer-reviewed outlets, including *New Media & Society*, *Journal of Cyber Policy*, *First Monday*, *Intelligence and National Security*, *Terrorism and Political Violence*, and *Studies in Conflict and Terrorism*, among others. He is the co-author, with Fen Osler Hampson, of *Look Who's Watching: Surveillance, Treachery and Trust Online* (CIGI Press, 2016).

Acronyms and Abbreviations

CIPA	Classified Information Procedures Act
CPU	central processing unit
CSLI	cell-site location information
FBI	Federal Bureau of Investigation
GPU	graphics processing unit
IP	internet protocol
ISPs	internet service providers
MAC	media access control
NITs	network investigative techniques
Tor	The Onion Router
VPNs	virtual private networks

Executive Summary

The dark web allows for anonymous browsing and publishing of content and is inherently cross-border by design. Law enforcement's best tool to police anonymous dark web sites is a suite of technologies known as "network investigative techniques" (NITs), which essentially hack The Onion Router (Tor) hidden services (i.e., darknet sites) to de-anonymize users. Using Operation Pacifier, the Federal Bureau of Investigation's (FBI's) 2015 investigation of the Playpen child abuse content darknet site, as a case study, this paper explores the implications of the use of NITs and both the Fourth and Sixth Amendments. We find that initial conflicts between the rules governing search and seizure and the search of machines using the dark web have been reconciled with changes to law and evolving legal precedent. The issues surrounding the due process remain more open.

Introduction

In 2015, the FBI took down a darknet child abuse content site called Playpen. At the time of its closure, the site reportedly had some 215,000 users and hosted upwards of 117,000 posts involving the sexual abuse of children. Approximately 11,000 unique visitors reportedly frequented the site each week (Cox 2016a). Because dark web users are anonymous by design, the FBI resorted to an extraordinary measure to identify those producing and consuming child abuse content via the Playpen site. Over the course of 13 days in late February and early March 2015, the FBI ran the site and used this time to implant malware into the site's code that would travel back and infect users' machines. Overall, roughly 8,000 devices in 120 countries were infected (Cox 2016c). The operation eventually led to more than 350 arrests in the United States, including 25 producers of child abuse content (Department of Justice 2017).

Law enforcement can effectively police the dark web through a number of techniques (Chertoff 2017; Jardine 2015; Jardine, forthcoming 2021), but the most technologically intensive of these approaches — known more euphemistically as NITs — raise a number of legal quandaries as they collide with long-standing legal principles in liberal democratic regimes. A NIT, when used in the example discussed here, can be thought of as a technological tool used to bypass the anonymity-by-design of the dark web. Within the United States, the closure of the Playpen darknet site is a useful example of two collisions between law and the technology of the dark web: the search and seizure devices that are using Tor and the Fourth Amendment; and the use of NITs and the Sixth Amendment.

This case and its associated challenges point to an ever-evolving problem of law and technology. The dark web is now a common platform for criminal activity, especially in liberal democratic regimes (Jardine, Lindner and Owenson 2020). The anonymity of the system gives rise to emergent use as a host of terrorist sites, gun marketplaces, drug bazaars, malicious software fora and pernicious child abuse content boards (Chertoff and Simon 2015; Moore and Rid 2016; Owen and Savage 2015; Topor 2019). Finding ways to minimize the excesses of the dark web through active law enforcement engagement, while also preserving the legal bedrock of liberal democratic societies, is key.

This paper summarizes the basic technical functions of Tor and provides details of the Playpen case. It highlights, in particular, the legal challenges that emerged due to the use of a NIT, teasing apart a number of challenges that govern the issuance of warrants, the employment of NITs, and the balance of due process and investigatory effectiveness. The rest of the paper proceeds as follows. The first section provides a summary of the technical functions of Tor. The second section unpacks the history of the Playpen case in finer detail. The final sections then walk through each of the Fourth and Sixth Amendment legal issues that are raised by this case study, highlighting both the core issues at hand and how they have worked out thus far in practice and how they may evolve in the future.

A Short Technical Introduction to Tor

Tor is an online anonymity-granting system, with origins linked to the US government (Collier 2020; Gehl 2018; Jardine, Hampson and Rowlands 2021; Levine 2014; Levine 2018; Maréchal 2018). It includes a browser bundle that is publicly available for download from the Tor Project website. The browser makes users anonymous online by leveraging the Tor overlay network — a system of approximately 6,500 volunteer computers spread throughout the world. When using the Tor browser, a user's query is automatically encrypted and relayed through a series of randomized hops from an entry point (guard node) to an exit node, which retrieves, through an unencrypted connection, the content a user wishes to consume (see Figure 1). Settings within the Tor browser bundle allow users to disable javascript.

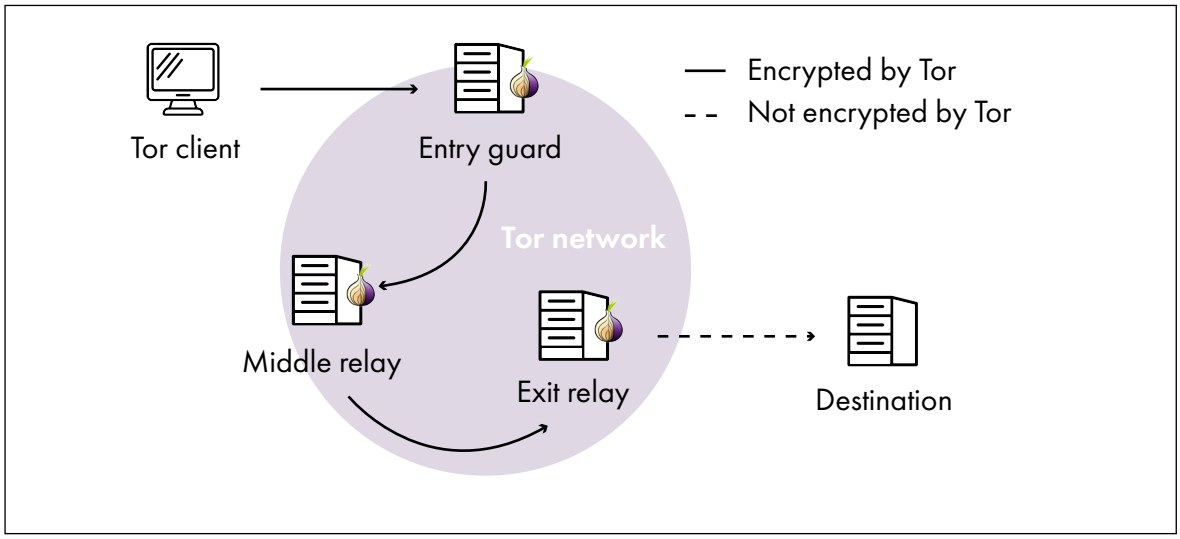
The net effect of this simple process of encrypted, randomized hops is that a Tor user becomes anonymous when online. Anonymity, in this sense, means only that a user's identity is disassociated from their actions (that is, the content they are publishing or consuming). Those operating the different parts of the Tor network might know either a user's identity (as proxied by an internet protocol [IP] address) or the content that is being viewed. But, by design, it is challenging for any single actor to be able to link a particular user with their actions.

A user's internet service providers (ISPs) or an entry node operator at the front end of the Tor network, for example, could know the IP address and geolocation of a device using the Tor network. But, because the content of the query is encrypted and the early nodes simply relay a query to the next randomly selected node in the chain, those in the front portion of the network can only know the user but not what they are doing with Tor. Conversely, exit node operators and those managing the servers that host the content that a user wishes to view can see what is being done. However, those at the end point of the system are hard-pressed to trace the origin of these activities back to a particular IP address, device or geolocation.

The Tor browser allows for reader anonymity (Gehl 2018), but Tor also provides anonymity to publishers (those who wish to set up and run dark web sites). Onion services, as these sites are known, make up the proverbial dark web, which can be usefully defined as "websites built with standard web technologies (HTML, CSS, server-side scripting languages, hosting software) that can be viewed with a standard web browser... which is routed through special routing software packages" (ibid., 5). If correctly configured, onion services (which were previously known during the tenure of the case study below as hidden services) are hosted and administered anonymously, so that those viewing the site cannot readily determine the physical location of the server hosting the content or the location of site administrators.

Tor does contain some weaknesses. As a low-latency anonymity network, large government agencies, for example, can probabilistically de-anonymize blocks of traffic by controlling large portions of both sides of the network (Johnson et al. 2013; Nurmi and Niemelä 2017). Additionally, prior investigations into darknet drug crypto markets show that manipulating server-side script on commandeered onion services can collect a host of data from users, as was done during the Dutch High-Tech Crime Unit's investigation into the Hansa darknet market in 2018 (Jardine, forthcoming 2021). Other vulnerabilities specific to the Tor platform may potentially exist and be known to major government agencies (Levine 2014; 2018). Despite these limits, the system generates fairly robust online anonymity for both consumers and producers of content, epitomized in the pairing of the Tor browser and Tor onion services (Dingledine, Mathewson and Syverson 2004; Gehl 2018; Moore and Rid 2016).

Figure 1: Anonymity Through Hops: Tor's Relay System in Action



Data source: Winter (2017).

The Playpen Case

The original indictments referred to Playpen simply as "Website A" (Raymond 2015). Alex Schreiber, a former math teacher from Queens, New York, was one of the first to be charged. According to the court filing, Schreiber — under the screen handle "philsic" — allegedly spent upwards of 194 hours on "Website A" from September 2014 to March 2015. During this time, he reportedly viewed child abuse content involving children as young as five years of age (ibid.).

"Website A" would later be identified as Playpen, a child abuse imagery bulletin forum hosted on a Tor onion/hidden service. While Tor has a number of legitimate privacy and censorship-circumvention functions (Jardine 2018a; 2018b), child abuse fora such as Playpen are an all-too-common and recurrent feature of the Tor network. Indeed, the storied history of Tor includes a number of examples of frequently trafficked darknet child abuse sites that provide an overarching context to Playpen's emergence and use. In the early 2010s, for example, Freedom Hosting, run by a man named Eric Eoin Marques, provided anonymous hosting for a number of Tor onion services. At the time, more than 100 child abuse imagery sites were located on Freedom Hosting's servers. This collection of sites reportedly accounted for as much as 95 percent of then-available dark web child abuse content (Poulsen 2013).

In a wider perspective, dark web child abuse sites routinely amount to both a small proportion of the overall available onion service content and a disproportionately large share of site visits/traffic. One study by Gareth Owen and Nick Savage (2015), for example, categorized thousands of onion services over a six-month period, placing them into thematic buckets. Consistent with other indexing efforts (Faizan and Khan 2019), Owen and Savage found that drug sites accounted for the largest plurality of categorized sites, followed by market sites, fraud sites and sites related to the cryptocurrency bitcoin (Owen and Savage 2015). Abuse content sites during this observation period accounted for around two percent of the total share of categorized onion services content. However, this small proportion of available content received more than 80 percent of the incoming site visits. As the authors of the study concluded, "Child abuse content is the most popular type of content on the Tor Dark Net" (ibid., 9).

The Playpen site fits into this wider pattern of Tor dark web content. At its height, Playpen had some 215,000 users. As a bulletin board site, these hundreds of thousands of users deposited upwards of 117,000 posts, most of which involved the clear sexual exploitation of children. The FBI affidavit that accompanied the original warrant to employ the NIT on visitors to the Playpen site

detailed the content of the bulletin forum in great detail. The site contained various forms of child abuse content, from tips on ways to safely access posts to a variety of discrete child abuse content types, with offerings in numerous languages other than English.[1] Playpen was reportedly receiving upwards of 11,000 unique visitors each week and likely many more returning visitors (Cox 2016a).

In December 2014, an undisclosed foreign law enforcement agency informed the FBI that the server upon which Playpen was running was misconfigured. While Tor normally hides the IP address of the servers running onion services, making it difficult to pinpoint the physical location of the server, the Playpen site was leaking a real IP address due to an initially undisclosed configuration error that later turned out to involve a default setting on the hosting web server (Cox 2016b). Using public lookups, the FBI determined that the IP address in question resolved to a server operated by Centrilogic, a private firm in Lenoir, North Carolina. The FBI then secured a warrant that allowed them to seize the server and commandeer the site. With the approval of several top-level officials within both the FBI and the Department of Justice (Cox 2017), the FBI migrated the site from the Centrilogic server to one run by the FBI based in Newington, Virginia. The FBI then operated the site for 13 consecutive days, from February 20 to March 4, 2015.

For the FBI, those 13 days had a clear investigative purpose. To circumvent the usual anonymity provided by Tor (Dingledine, Mathewson and Syverson 2004), the FBI aimed to infect the machines of visitors to Playpen with a NIT, which is, essentially, malware. The accompanying affidavit to the warrant application indicates that there was probable cause to believe that those accessing Playpen were engaging in:

- child exploitation (a violation under 18 US Code, section 2252A(g));
- the possession of child abuse imagery (a violation under 18 US Code, sections 2252A(a)(5)(B) and (b)(2));
- the advertising of and conspiracy to advertise child abuse content (a violation under 18 US Code, sections 2251(d)(1) and (e));
- and receiving child abuse content (a violation under 18 US Code, sections 2252A(a)(2)(A) and (b)(1)).[2]

Given the affirmative steps needed to access darknet .onion sites (they cannot be stumbled upon from, say, Google), the long litany of violations makes clear that visitors to Playpen were intending to view, share or otherwise discuss and engage with child abuse content. Objections to the FBI's course were later raised, most notably that this policy could inadvertently lead to the effective revictimization of children (Yung 2016). Yet, as FBI Special Agent Daniel Alfin noted, "Without going forward with this operation, we would have had no capability to identify anyone other than the creator of the Playpen website" (Cox 2017).

Magistrate Judge Theresa Buchanan issued the warrant to employ a NIT to search visiting machines on February 20, 2015. Using the NIT, upwards of 8,000 unique machines were identified globally, followed by hundreds of arrests. Crucially, while separate residential warrants were issued to search homes across the United States, all of the initial 8,000 or more machine-level searches emanated from this single warrant authorized in the Eastern District of Virginia (Cox 2016c).

The case ultimately became extraordinarily contentious. Two issues emerged as particularly controversial in the wake of arrests stemming from the warrant: issues of privacy and jurisdiction (embroiling the Fourth Amendment) and issues of due process and investigatory method (Sixth Amendment).

1 See Case No. 1:15-SW-89, *Search and Seizure Warrant in the Matter of the Search of Computers that Access upf45jv3bziuctml.onion*, (ED Va 2015).

2 *Ibid*.

Search and Seizure and the Fourth Amendment

The modern state holds a near monopoly on the legitimate use of force (Weber 2004). With its primacy within a given set of territorial borders, the state and its coercive arms are often an incredibly powerful force. Early liberal political theory in both Britain (Locke 1796) and the United States (de Tocqueville 2004) was deeply concerned with how best to limit the immense power of the budding modern bureaucratic state. Failure to do so meant the potential for governmental overreach, excess and abuse.

Within the liberal democratic tradition, the rule of law became a primary restriction on the potential power of government. Rules that are publicly known and consistently applied were to bind governments to prevent their excesses. These restrictions took, and continue to take, a number of different forms. One premier example is that of rules governing search and seizure by governments. British parliamentarian William Pitt summed up the principle nicely in an address to Parliament in 1763: "The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter, the rain may enter, but the King of England may not" (Pitt, quoted in Levy 1999, 80).

As in England, so too in America. A series of intellectual debates, political events (such as the general warrant issued in the case of newspaper editor John Wilkes and *The North Briton* No. 45 in the colonies), and a host of other forces eventually culminated in the Fourth Amendment of the US Constitution. The final text of the amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Fourth Amendment protects individuals within the United States from unreasonable search and seizure. Implementation of the principles embedded in the Fourth Amendment is guided by Rule 41 of the Federal Rules of Criminal Procedure. The rule precisely specifies when, and over what, judges are allowed to authorize search warrants. Rule 41(b) details the venue for a warrant application in great detail. In 2015, at the time of the Playpen investigation, Rule 41(b)(1) authorized a magistrate judge "to issue a warrant to search for and seize a person or property located *within the district*."[3] While other sections of Rule 41(b) allow for the issuance of warrants outside of the magistrate judge's district when the investigation involves international terrorism (b)(3), the use of tracking devices (b)(4) or a number of specific circumstances involving territorial embassies and US territorial possessions (b)(5), similarly explicit provision was not made in cases of child abuse imagery or for crimes involving the internet or dark web that defy traditional notions of geography and jurisdiction.

The absence of such an exception was the rub. The warrant authorizing the Playpen investigation using a NIT was at variance with Rule 41(b) as it existed in 2015. The NIT warrant in the Playpen case was issued to cover the search of machines "wherever located," yet Magistrate Judge Buchanan could only, given the state of the Federal Rules of Criminal Procedure at the time, legitimately authorize a search of devices located within the Eastern District of Virginia. The mismatch between legal rules and the technology of Tor — which is inherently cross-border, at least in its potential — resulted in a number of significant legal battles.

One exemplifying case is the government indictment of Alex Levin, a Massachusetts man charged with possession of child abuse imagery in relation to the FBI's Playpen investigation. The FBI's NIT determined that a user with the screen handle of "Manakaralupa" was accessing child abuse content in March 2015. The user's machine traced back to Levin's physical address in Norwood, Massachusetts. On August 11, 2015, law enforcement obtained a residential warrant issued by Magistrate Judge Marianne Bowler to search Levin's home. There they found sufficient evidence to charge Levin with possession of child abuse content.[4]

As part of his defence, Levin argued that the evidence stemming from the search conducted under the NIT warrant should be suppressed,

3 US, Committee on the Judiciary, House of Representatives, 116th Cong, *Federal Rules of Criminal Procedure* (2020) at rule 41 [*Rules of Criminal Procedure*], online: <https://www.uscourts.gov/sites/default/files/federal_rules_of_criminal_procedure_-_december_2020_0.pdf>. (Emphasis added.)

4 *United States v Levin* (1st Cir 2016).

charging that the initial warrant itself was invalid. The case was heard by Judge William G. Young in the District of Massachusetts. The court ruled that, due to violations of Rule 41(b)(1), the initial warrant was indeed invalid *ab initio* (from the beginning). As Judge Young wrote in his ruling, "Because the NIT Warrant purported to authorize a search of property located outside the Eastern District of Virginia, and because none of the exceptions to the general territorial limitation of Rule 41(b)(1) applies, the Court holds that the magistrate judge lacked authority under Rule 41(b) to issue the NIT warrant."[5] Judge Young also determined that no additional "good faith exceptions" reasonably applied and the evidence against Levin stemming from the NIT was to be suppressed.

The government appealed the district court's conclusion. The First Circuit Court of Appeals heard the case in October 2017 and overturned Judge Young's decision. The appeals court found that while the search might have resulted in a technical violation of Rule 41(b), the fault — if any — was that of Magistrate Judge Buchanan and not that of the FBI. The law enforcement officers who conducted the search of Levin's computers with the NIT acted in good faith by assuming that the warrant was lawful. Writing for the court, Circuit Judge Juan Torruella presented the appeals court's rationale as follows: "The officers acted pursuant to the warrant....[T]he executing officers had no reason to suppose that a mistake had been made and the warrant was invalid....[T]he NIT warrant was not written in general terms that would have signaled to a reasonable officer that something was amiss. The warrant in this case was particular enough to infer that, in executing it, 'the [executing officers] act[ed] with an objectively 'reasonable good-faith belief' that their conduct [was] lawful."[6]

Legal battles similar to those surrounding the Levin case played out in multiple circuit courts in the wake of the Playpen investigation. Gradually, a consensus emerged that the NIT warrant might have been a technical violation of Rule 41(b) as it existed at the time, but the ensuing searches were nevertheless made in good faith. As a result, the evidence against the various defendants in the wider Playpen case was generally upheld. Similar to the events in the First Circuit Court of Appeals, for example, both the Eighth and the Tenth Circuit Courts of Appeals reversed lower court rulings suppressing the evidence from the NIT warrant.[7] In the Seventh and the Ninth Circuit Courts, the appeals courts upheld lower district court rulings that declined to suppress evidence from the NIT investigation, arguing that the searches were made in good faith.[8]

The collision of technology and law governing search and seizure that emerged in this case was so foundational to the structure of policing Tor with NITs that it also gave rise to a subsequent revision to the Federal Rules of Criminal Procedure. In its current iteration, Rule 41(b)(6) now contains an important caveat reconciling the anonymous nature of the dark web with the requirements of law in the United States. A magistrate judge can now issue a search warrant for an electronic device when there is evidence that some part of the criminal activity occurred in their district and "the district where the media or information is located has been concealed through technological means."[9] While commercial tools such as virtual private networks (VPNs) also provide a degree of anonymity that would imply users of these tools also fall under the expanded provision, the technology of the dark web is, by design and function, a robust technological means of concealing location.

These revisions to Rule 41 discretely resolve one initial legal controversy inherent to the issuance of a warrant authorizing the use of a NIT for the search and seizure of information on machines accessing the Playpen dark web site. How the tension has been resolved in the US context, however, generates its own set of tensions between liberal democratic principles of law regarding allowable search and seizure, sovereignty and the technology of the dark web, including issues of technical definitions, potential venue shopping and wider jurisdictional concerns.

5 *Ibid.*

6 *United States v Levin*, 874 F (3d) 316 (1st Cir 2017).

7 *United States v Andrew Joseph Workman* (10th Cir 2017); *United States, Appellant v Steven Shane Horton and Beau Brandon Croghan* (8th Cir 2016).

8 *United States v Kienast*, 907 F (3d) 522 (7th Cir 2018); *United States v Henderson*, 906 F (3d) 1109 (9th Cir 2018).

9 *Rules of Criminal Procedure*, *supra* note 3 at rule 16.

Search and Seizure and Technical Definitions

One issue raised by the expansion of Rule 41(b) is a definitional question about the nature of technological obfuscation online. Preventing abuse of the new provisions becomes key. The issue of technological masking of physical location can be thought of on two levels. The first is the somewhat simpler case evident in the Playpen investigation. In this case, the site that the FBI was using as a delivery vector for the NIT was set up using Tor (an onion/hidden service), making the site accessible only to those using the anonymizing Tor browser or a similar browser employing special routing software (Dingledine, Mathewson and Syverson 2004; Gehl 2018). By implication, a regular internet user employing a web browser such as Chrome could not accidentally stumble upon the site. Evidence of visiting a Tor onion service (a .onion domain) can, therefore, be taken as *prima facie* evidence of using the Tor browser (or a similarly routed browser) to mask one's IP address and location through technological means. Narrowly defined dark web investigations that focus on Tor crypto markets or child abuse sites hosted on onion services easily satisfy the new exception to Rule 41(b).

Second, the expansion of Rule 41(b) also covers the possible use of the Tor browser as a surface web navigation tool, creating a wider potential application of the new exception outside of darknet (i.e., .onion site) investigations. According to one recent empirical investigation, around 7.8 percent of Tor network clients in liberal democracies on an average day use the system to access onion services. The remainder use the Tor browser to engage with surface web content (Jardine, Lindner and Owenson 2020). The implication is that the expansion to Rule 41(b) could, therefore, apply to criminal investigations not on the putative darknet, but on the regular Web as well, if sufficient evidence could be marshalled to say that the Tor browser bundle was being used.

In these cases, the burden of proof necessary to secure a warrant under the exemption hinges on the sort of evidence that can show use of the Tor network to mask the original IP address and location of the user in question. Because of Tor's routing system, the observation that malicious activity is emanating from a known exit node address implies that technological obfuscation steps are being used by the unknown initiator of that traffic. Compiling a list of known exit node addresses could be an efficient step toward an easy diagnostic method for determining if Tor is being used to mask locational information.

Yet this sort of approach is sensitive to false negatives. New Tor exit node addresses may not currently exist on law enforcement's copy of the Tor exit node list, obscuring the use of technological masking tools. Additionally, the tracking of exit nodes might also prompt counter-responses. The Tor Project, for example, might adapt to this threshold of evidence by publishing a smaller proportion of exit nodes on Tor directory sites or using additional non-public bridges on the exit side of the network — which add a hop — to reach content without revealing to the website operator or law enforcement that the Tor network has been used.

Independent of what law enforcement does in this regard, developments in the commercial space might also increase the likelihood that the Tor Project will make a more concerted effort to obfuscate exit node traffic. For example, the content delivery network CloudFlare imposed CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) on all traffic leaving known Tor exit nodes in 2016, as much was deemed to be potentially malicious (Prince 2016).

For now, traffic coming from a known exit node address can be taken as evidence of the use of the Tor network, but a number of steps can be taken that undermine the comprehensiveness of this method of determining when the new jurisdictional exception to Rule 41(b) should apply. Absent evidence of activity on discrete onion services or use of the Tor network (or similar technologies on I2P or Freenet) to engage with content, attempts to justify potentially extra-jurisdictional searches via the revised Rule 41(b) should be met with some skepticism.

Search and Seizure and Expectations of Online Privacy

Definitional questions about what constitutes the use of masking technology also raises a more fundamental question about the nature of private or public information online. Implicit in the issuance of a warrant under the Fourth Amendment is the idea that the information or location to be searched is private. But not all information is private; some, as legal precedent suggests, is inherently public.

One example of this sort of debate is the issue of the public or private nature of IP addresses. IP addresses are one of the fundamental building blocks of the internet. While these numbers can be easily spoofed, they are, in practice, session-unique identifiers assigned to a machine by an ISP when a person goes online. An IP address is used in web communication, operating essentially like a return address for communication between, say, a person and the website they are visiting.

Based on this technical structure, the court in *United States v. Forrester* (2007) decided that IP addresses were public information. In a routine web session, a person's ISP provides an address to a user and keeps a record of the accounts to which they assign an address. Likewise, the websites that a person visits use the IP address to record the origin of traffic and return queried content. In the legal decision rendering IP addresses public information, the Ninth Circuit Court of Appeals decided that "Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[10] Other cases after *Forrester* reached similar views on the public nature of IP address information (Sartain 2013). The reasoning found in *Forrester* has been used in judicial proceedings to justify dark web searches, both in the case of *United States v. Farrell*[11] involving the drug crypto market Silk Road 2.0 and *United States v. Michaud*[12] during the Playpen investigation.

While the view that IP addresses are public remains contested in new legislations such as the California Consumer Protection Act, the general lesson that IP addresses are not private, and so are not something governed by Fourth Amendment standards, continues to be supported by new judicial decisions following *Carpenter v. United States* (2018).[13] *Carpenter* challenged third-party doctrine, or the idea that information that a user voluntarily shares with a third party in the use of their service is not private by definition, and raised issues of the right to privacy of movement and location, which had previously been upheld in cases of GPS data.[14] In particular, the case took up the issue of geolocation and cell-site location information (CSLI), which are the details that are broadcast from mobile devices to the cellular towers that provide call and internet access. Despite the potential for this ruling to revise how IP addresses are viewed in legal terms, since IP addresses, unmasked by technological means, do broadcast location information to third parties, the balance of opinion since *Carpenter* has shown that IP addresses remain public information under US law. *Carpenter*, then, more narrowly applies to constantly or repeatedly broadcast locational information and broadly formulated searches. Specific searches for location or metadata (data about data), such as session-specific material like IP addresses, do not necessarily reach the privacy thresholds set in *Carpenter*.[15]

From an investigative standpoint, extensions of the legal logic found in *Forrester* and *Carpenter* could expand the types of informational content deemed public. The legal reasoning at work in these cases hinges on four factors. The first is the functionality of IP addresses within the process of internet activity. Unless tools such as VPNs or the dark web are used, a person's IP address is regularly shared and collected by the websites they visit. Second, users voluntarily share IP information by knowingly visiting a site. Third, IP addresses are metadata and not content, so the potential invasiveness of this sort of data collection may be lessened in some cases — even though very detailed profiles of users and their activity can be constructed from metadata alone (Schneier 2015). Finally, the interpretation surrounding CSLI following from *Carpenter* suggests that information that is both shared routinely with third parties and, more or less, constantly broadcast could be considered private, but information that is time-delimited or session-specific is not subject to the same Fourth Amendment protections.

The legal logic of these cases could suggest that other types of data that law enforcement might collect during a dark web investigation might likewise be nominally public and not private information. Cookies as a collection mechanism are a prime example. Cookies are bits of code — not so dissimilar, potentially, to the NIT used by the FBI

10 *United States v Forrester*, 512 F (3d) (9th Cir 2007) [*Forrester*].

11 *United States v Farrell*, 606 F (2d) (2016).

12 *United States v Michaud* (2015) [*Michaud*].

13 *Carpenter v United States*, 138 S Ct 2206 (2018).

14 *United States v Jones*, 565 US 400 (2012).

15 *United States v Hood* (1st Cir 2019); *United States v Kidd*, 394 F Supp (3d) 357 (SDNY 2019); *United States v Vandyck* (9th Cir 2019).

in the Playpen case — that download to a person's device when they view a website. Cookies can be persistent or session specific. They are a ubiquitous technical feature of the Web and serve a number of useful functions, such as allowing people to move between webpages while maintaining a shopping cart full of items on e-commerce sites. Cookies collect a lot of information, such as a record of a site visitor's operating system, browser type, battery life, monitor size, and details about both the central processing unit (CPU) and the graphics processing unit (GPU) of the visiting machine. Cookie collection, in other words, is a common function of an individual's web-based activity, can be tailored to collect only metadata and not content, is often voluntarily given to website operators through the act of using the site, and can be time delimited, at least in the case of session-specific cookies that disappear after a browser session is complete. Within some limits, the legal reasoning and precedent from *Forrester* and *Carpenter* might apply, even as legislative rules have become stricter about regular web cookie use in jurisdictions such as the European Union.

The possibility that what cookies collect might be public information could have profound implications for future dark web investigations. Cookies do not collect all the details, such as a media access control (MAC) address or host name of the device, that were gathered by the FBI's NIT in the Playpen case. However, much of the other informational content that cookies do routinely collect is mirrored in the data collected by the Playpen NIT, such as details on the device's operating system. Expansion of legal precedent to render the data collected by cookies as public could potentially allow law enforcement to sidestep the Fourth Amendment issues stemming from the use of NITs. Law enforcement might, in the event, collect less information overall but do so without the need for a warrant as the information that is collected when running a site could arguably be public, not private.

For example, based on an expansion of the information covered by *Forrester* and *Carpenter*, law enforcement could potentially collect both an IP address and operating system details without needing a warrant. From this information, a targeted residential warrant could later be pursued that could detail both the location and address of the offending machine based on the IP address of the visiting computer and the type of machine that visited the site, down to the operating system (for example, Windows 10) and GPU and CPU models and versions. This level of information would allow law enforcement to specify precise locational and device-level details for a later search warrant from an initial warrantless collection of potentially public information.

Of course, expansion of the precedent of *Forrester* and *Carpenter* to other web content and tracking tools is not without problems. Three factors, in particular, potentially militate against such an expansion of the legal reasoning. First, there may be relevant agential differences at play. Sharing an IP address by visiting a site and having your information collected by cookies are not necessarily equivalent processes. For a website or ISP to record an IP address visiting a certain site, the user behind the IP address must enter the website address they wish to visit into a search bar or otherwise decide to visit the site by clicking a hyperlink. Framed differently, the user chooses to visit the site and thus shares their IP address with the operator as a fundamental step in that process. In contrast, cookies are important — but not essential — additions that website operators can choose to deploy to track information about their users. The locus of agency varies between these two examples. In the first, the user decides which sites to visit. In the second, the choice to collect user information becomes the prerogative of the website operator who opts to deploy cookies. Cookies may be ubiquitous and collect information that plays an important function in the operation of the contemporary Web, but the locus of choice that results in the collection of information matters.

Second, a definition of public and private information should be nested within a wider context of both technological development and social processes. An important distinction can be drawn between information that is shared as an inherent function of online activity (such as IP addresses) and information that is collected via cookies due to the commercialization of the Web (Zuboff 2019). IP infrastructure is generative (Zittrain 2008) in the sense that it provides an essential interoperable platform on top of which a lot of innovation can occur. Cookies, on the other hand, are discretely useful, especially for e-commerce and web-based advertising, but are not a necessary component of broad categories of online activity in the same way as IP addresses. A burden of necessity seems to suggest that sharing

one type of information (that is, IP addresses) could be considered public information because it must be shared during online activity (although it can be masked or spoofed), while other information (for example, operating system details collected by cookies) may be useful information for operators to know but is often not necessary.

Lastly, and more germane to the application of the *Forrester* decision to dark web investigations as was done in *Farrell* and *Michaud*, the search in the *Forrester* case presented no Fourth Amendment issues since "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[16] This reasoning remains valid with regard to normal internet activity, but use of obfuscation technologies such as the dark web (or simpler tools such as commercial VPNs) somewhat complicates the logic. The dark web provides anonymity by disassociating a person's IP address assigned for a session by their ISP from the content they are viewing. Such a disassociation entails that Tor users are quite purposefully not turning over their real IP addresses to website operators, nor allowing their ISP to construct a record of which sites they are visiting. In other words, when using the dark web, users might, to reverse the logic of the *Forrester* decision, have a legitimate expectation of privacy because they are not voluntarily turning over their address information to third parties. Since the Tor browser can also be run without javascript, it is reasonable to say that Tor users are taking affirmative steps to make what is sometimes public information private, and that might imply differing legal standards. Broadly, this objection would imply that the legal reasoning in *Katz v. United States* and *Smith v. Maryland*, where people can have a reasonable expectation of privacy in certain domains or for certain types of information if society widely agrees it to be the case, might override the points made in *Forrester*.[17]

Search and Seizure and Venue Shopping

Beyond evidence of masking tools at play, the revised Rule 41(b) also requires that some aspect of the crime be happening in the jurisdiction within which the warrant application is filed. For darknet crimes involving onion services, this requirement can be easily satisfied given that law enforcement can theoretically migrate a site to servers located in any territorial jurisdiction, especially in cases such as those involving child abuse content where accessing the content itself is illegal. Given this ability to pick the location of a crime, law enforcement could deliberately move the (server) location of the criminal content to a favourable setting to circumvent magistrates with a history of requiring higher thresholds of evidence.

Plausibly, standards of probable cause in dark web–related cases could be set by the most amenable district magistrate opinions. If the Playpen case were to be investigated today under current rules of criminal procedure, the FBI could move the site from Lenoir, North Carolina, to the most favourable district in the United States, based on an admixture of needed infrastructure to host the content and an FBI presence. Such a move would satisfy both the evidence of masking and the single element of a crime criteria in one swoop. Given the ease with which a simple migration could satisfy the exemptions to the revised Rule 41(b), migrating the site to those locations deemed favourable to a law enforcement warrant request could become an additional feature in the calculus.

Search and Seizure and International Jurisdiction

The fourth outstanding point regarding search and seizure involves the wider jurisdictional issues that emerge from investigating inherently cross-border technologies such as the dark web. Revisions to Rule 41(b)(6) effectively make new allowances for extra-district searches authorized by a magistrate judge when technologies such as Tor are used to mask the location and identity of a user. However, the technologies of the internet and the dark web are global, not territorially bounded by national borders. Indeed, in the Playpen case, upwards of 8,000 real IP addresses in 120 countries were searched, all as a result of the single NIT warrant issued in the Eastern District of Virginia (Cox 2016c). Only a few hundred suspects were identified within the United States (ibid.).

16 *Forrester, supra* note 10.

17 *Katz v United States*, 389 US 347, 351; *Smith v Maryland*, 442 US 735, 740.

Certainly, not all cross-border investigations are going to give rise to negative foreign relations consequences (Kerr and Murphy 2017). Indeed, cross-border law enforcement collaboration is increasingly common for dark web crypto market takedowns and child abuse site investigations (FBI 2017). Yet the wider potential jurisdictional problem, given current law and the nature of dark web technologies, cannot be fully discounted (Ghappour 2017). Any warrant authorized by a magistrate judge within the United States to conduct digital searches of dark web users has an extraordinarily high chance of resulting in an effective search of non-US persons. These cross-border searches are indicative of wider jurisdictional issues generated by the internet and potentially challenge national sovereignty (Chertoff and Rosenzweig 2015). As Ahmed Ghappour (2017, 1098) notes, "The exercise of extraterritorial law enforcement functions will be unilateral. It will not be limited to matters of national security, nor will it be coordinated with the State Department or other relevant agencies. Case-by-case investigatory decisions made by rank-and-file officials will have direct overseas consequences." As the well-publicized, if transient, diplomatic fallout from the Edward Snowden disclosures makes clear, states can react negatively to electronic surveillance of their citizens by a foreign power.

Such consequences suggest the need for a continuation of wider collaboration on dark web policing efforts across borders (Kerr and Murphy 2017). Improvements in international cooperation on dark web policing can be had through a combination of incremental and voluntary legal harmonization and improvements to the mutual legal assistance treaty process, nested within a framework of reciprocity (Chertoff and Rosenzweig 2015). Such changes might help to resolve some of the lingering extra-jurisdictional challenges that are inevitable in a world of anonymity and globe-spanning networks.

The Dark Web, NITs and the Sixth Amendment

Privacy and jurisdictional considerations are not the only issues raised by dark web investigations. NITs are one of the most persistent public policy challenges of the dark web (Chertoff 2017). The deployment of NITs, as was the case in the FBI investigation of Playpen, often involves the exploitation of software vulnerabilities, much as is done by malicious hackers wanting to steal personally identifiable information from individuals, companies or governments. Once deployed, these tools provide law enforcement with exceptional access to targeted devices. Policing drug crypto markets, terrorist communication nodes or child abuse sites can still leverage traditional modes of detective work (Dolliver 2019; Jardine 2015; Jardine, forthcoming 2021; Norbutas 2018). But, unless drugs bought on the dark web are intercepted in transit, undercover agents get administrative access to a site through duplicity and deception, a misconfiguration of the server hosting the .onion address leaks real IP information or the criminal simply slips up, the most effective way for law enforcement to beat the technical protections of Tor is often to hack the technology itself. NITs provide a means of doing so.

While NITs are effective investigative tools, they also give rise to a number of legal quandaries as they intersect with due process statutory rights contained in Rule 16(f) of the Federal Rules of Criminal Procedure and the Sixth Amendment (Garcha 2018). In broad strokes, the Sixth Amendment aims to ensure a timely and fair trial for those facing criminal charges. Part and parcel of this guarantee are, in the language of the Sixth Amendment itself, the rights to be "informed of the nature and cause of the accusation" and "to be confronted with the witnesses against him." In practice, these provisions help to ensure that defendants can mount a reasonable legal defence.

Discovery allows defendants to learn what information and evidence the state intends to marshal against them. Knowledge of such information is integral to a successful legal defence in an adversarial legal system and a cornerstone of restraint on governmental power. As noted in Rule 16 of the Federal Rules of Criminal Procedure, "broad discovery contributes to the fair and efficient administration of criminal justice by providing the defendant with enough information to make an informed decision as to plea; by minimizing the undesirable effect of surprise at the trial; and by otherwise contributing to an accurate determination of the issue of guilt or innocence."[18]

Unlike evidence collected and used in more routine criminal investigations, the functional details of a NIT are integral to both successful legal defence in

18 *Rules of Criminal Procedure*, *supra* note 3 at rule 16.

the present and future law enforcement operations. On the one hand, knowledge of what the NIT did, when, for how long, and how it did its task is key to mounting a successful legal defence. On the other hand, the utility of a NIT, since it will involve exploits of code, is directly related to its publicness, with widespread knowledge of the exploit being inversely related to its usefulness in future law enforcement investigations. Given these tensions, the disclosure of a NIT in a criminal case is plausibly both necessary under the Sixth Amendment and associated statutory rights — although the form of disclosure is more open, as discussed below — and contrary to the potential effectiveness of that tool in future dark web investigations. Balancing the tensions between these two contradictory points requires attention to issues of NIT false positives and a bundle of issues involving discovery, disclosure and the value of NITs.

NIT False Positives

For a proper legal defence to be made in a case involving a NIT, the defence team will need to be able to ascertain the rough likelihood that a suspect was incorrectly identified. It is helpful to think about NITs as they were used in the Playpen case as similar to a witness in a regular, offline criminal case. A human witness may identify a potential suspect by commenting on the height, weight, hair colour and complexion of a person they saw committing a crime. Assessing the plausibility of these data points gives the defence (and jury) a sense of the accuracy of the classification. If the witness commented on these features yet was standing 60 metres away from the suspect at the time of the crime, the classification is in doubt. If, however, the witness was less than two metres away when the crime happened, then a positive identification of the suspect seems more plausible. Crucially, knowing the details of the identification process becomes paramount in assessing the validity of the classification.

Just like a human witness, machine classification systems can be incorrect in their assignment of individuals to categories. In more scientific terms, they all have what is known as a false positive rate, which means that the NIT used in the Playpen case could return to the servers run by the FBI an IP address, MAC address and other information that is not actually associated with a genuine user of the site. The police might then marshal evidence from the NIT to further investigate or even charge someone who is not actually involved with the abuse.

The issue is not so much that false positive rates exist, since they can never be completely eliminated, but that until you look at what the code of the NIT is doing and how it transmits information back to law enforcement, it is not possible to determine its accuracy level. Additionally, unlike well-documented forensic evidence-gathering methods such as DNA tests, which are repeatedly used and come with well-known risks of error, NITs more often tend toward limited-use cases. The implication is that an assessment of a NIT's risk of false positives in one case cannot illuminate much in terms of similar risks in future cases as the identification mode likely varies.

Two mechanisms might potentially lead to false positives in the use of NITs during dark web investigations. First, it is not impossible to think that a NIT could escape into the wild, depending on how it is designed and the occurrence of unintended adverse interactions once it is deployed. Such a lateral move could, for example, be localized. If there are multiple residents of a household sharing a single router, one person could visit the Playpen site, and the NIT could infect their machine but then potentially spill over and infect all machines using the same router. The spillover could also be broader if the malware is designed (intentionally or not) similar to a worm that propagates independently across systems.

The second pathway to a potential false positive involves the transmission of data from a target computer to law enforcement. The NIT in the Playpen case infected devices, for example, and then sent unencrypted information about those systems back to FBI-run servers. This transmission meant that data used to identify potential users of Playpen travelled over the open internet, allowing it to be potentially seen, intercepted or even tampered with by an intervening third party, through what is broadly known as a "man-in-the-middle attack" (Rose 2016). The possibility of such an attack raises questions about the chain of custody for crucial information used in the Playpen investigation and also injects the possibility of false positives into the equation at some unknown rate. Potentially, these sorts of concerns regarding false positives could rise to the level where they undermine the validity of any charges against those

identified by the NIT. Indeed, just such an argument about the integrity of the chain of custody was made by the legal defence team of Edward Joseph Matish III, who was charged in the Playpen case.[19]

Discovery, Disclosure and the Value of NITs

Given the general problem of false positives when using NITs, a full legal defence would plausibly need to know what the code of a NIT says, how it is designed, what it is meant to do, what it exploits, and whether it may be prone to false positives, unintentional distribution, or unencrypted communication and chain of custody issues. The Sixth Amendment and statutory rights to discovery, in other words, might require that the government disclose to defendants the interworking of their investigative tools.

The trouble here is that NITs — probably one of the most effective dark web investigative tools in law enforcement's tool kit — are often expensive to develop, limited in number and, most importantly, much less effective if publicly known. More generally, NITs used to police the dark web are also inherently useful across domains. As Susan Hennessey and Nicholas Weaver (2016) put it, NITs "are comprised of hundreds or thousands of lines of code, much of which is implicated in highly sensitive law enforcement, military, and intelligence activity. So a compromise to one small part of an exploit could harm a vast array of incredibly important national interests." Framed differently, defendants might have the right to examine the code used to identify them, but government has an incentive to withhold disclosure to protect their asset, retaining it for future use.

These differing incentives can give rise to familiar "graymailing" scenarios. Recognizing the government's incentives and the protections of the Sixth Amendment, legal defence teams may try to pressure the government to drop the charges rather than disclose the inner workings of their NIT (Garcha 2018). More precisely, graymailing is a practice wherein the defence attempts to either introduce classified information into a case or, alternatively, compel the disclosure of classified information by the prosecution (Liu and Garvey 2012). While not all NITs necessarily employ classified systems, the general idea is to get the government to drop charges rather than reveal the details of a tool used in a given case.

During the Playpen investigation, several legal teams attempted to, effectively in some instances, graymail the government into dropping the criminal charges by asking to see the details of the NIT. Matish's legal defence team attempted such a manoeuvre, for example, but was denied by the court.[20] The legal team defending Jay Michaud, however, was far more successful. The details of the case exemplify the conflict between the Sixth Amendment and statutory rights under Rule 16 of the Federal Rules of Criminal Procedure and the sensitive, finite, and useful nature of NITs for both dark web investigations and a wider gamut of law enforcement and intelligence community activities.

Michaud frequented Playpen under the screen name Pewter. As detailed in the initial criminal complaint, Pewter spent a total of 99 hours logged in to Playpen from October 31, 2014, when he initially joined the site, to March 2, 2015. During this time, he allegedly viewed 187 threads on a variety of subjects involving the sexual exploitation of boys and girls under the age of 11. During the 13-day period when the FBI was directly controlling Playpen in late February and early March 2015, Pewter was active on the site on seven separate days.[21]

While lodging a Fourth Amendment challenge questioning the initial legality of the search warrant, Michaud's defence team also filed a discovery request pursuant to Rule 16(d) of the Federal Rules of Criminal Procedure. Mirroring many of the rationales above, the defence stated, "The defense is seeking a copy of the code [of the NIT] so that its computer forensics expert can independently determine the full extent of the information the Government seized from Mr. Michaud's computer when it deployed the NIT; whether the NIT interfered with or compromised any data or computer functions; and whether the Government's representations about how the NIT works in its warrant applications were complete and accurate."[22]

The defence additionally offered to enter into a protective order to limit who could access the

19 *United States v Matish*, 193 F Supp (3d) 585 (ED Va 2016).

20 *Ibid*.

21 *Michaud, supra* note 12.

22 Motion to Compel Discovery, *United States v Michaud* (WD Wash 2015).

code in order to assuage some of the government's concerns about public disclosure. Illustrating the sensitive nature of the NIT, the government declined to turn over the code. It quickly filed its response to the motion to compel, documenting both the extent to which they had already shared a variety of pertinent information with the defence and law enforcement privilege as a protection against disclosing the full code behind the NIT.[23]

The court ruled in favour of the defence and compelled the full disclosure of the NIT. The government, calculating the benefits and costs of disclosure, dropped the charges against Michaud (Garcha 2018). As federal prosecutor Annette Hayes wrote in the court filing dismissing the case, "Because the government remains unwilling to disclose certain discovery related to the FBI's deployment of a 'Network Investigative Technique' ('NIT') as part of its investigation into the Playpen child pornography site, the government has no choice but to seek dismissal of the indictment" (Newman 2017).

Solving the tensions surrounding NITs can both look backward to existing processes and forward to revised frameworks (Garcha 2018). Peering backward, previous graymail cases in other domains gave rise to the Classified Information Procedures Act (CIPA), which contains useful rules to govern the discovery process such as potential government redactions of text from classified material, descriptive summaries in the place of real content and the possibility of *ex parte* and in camera reviews of evidence (Liu and Garvey 2012).

At the same time, the application of previous rules must accommodate the highly technical nature of NITs (Hennessey and Weaver 2016). The judge in *Michaud* compelled full disclosure, for example, but also reportedly acknowledged that some of the technical issues involved with both evaluating a NIT and fully assessing the potential impacts of disclosure were outside his area of expertise (Newman 2017). Likewise, plain-text descriptions of what code is supposed to do are not fundamentally equivalent to a direct review of the code itself or tests to see what code actually does in practice. Indeed, the whole point of compelling disclosure is that a NIT, as a computer program, might behave in unintended ways, just as any other block of code might do. Because of the inherently technical nature of the systems involved, certain provisions in CIPA, therefore, are less applicable to NITs than to, say, the classified text of government documents, memoranda or witness statements.

There is also a chance that persistent graymailing of government cases involving NIT use on the dark web might give rise to more extensive public-private partnerships that could circumvent defendant rights to discovery (Garcha 2018). Often, the property interests of the companies prevail when trade secrets collide with rights of discovery, even in criminal proceedings (Wexler 2018). Persistent, recurring decisions to compel disclosure of government NITs used in dark web investigations could, therefore, lead to a substitution of work effort from government to industry. The effect of such a move might be to give law enforcement tools more longevity, but it could also weaken individual rights to view the evidence (and the source of evidence) being used in a criminal proceeding.

Conclusion

The dark web is often used as a platform for criminal misdeeds. Child abuse imagery sites are one of the most popular types of Tor dark web content (Owen and Savage 2015). Law enforcement actively polices these sites, but these investigations can give rise to numerous tensions between investigatory technologies and existing law and legal precedent. Operation Pacifier, the FBI's 2015 investigation that resulted in the takedown of Playpen, is indicative. While public opinion, law and policy continue to evolve in ways that can address some of the controversies at hand, many lingering issues remain.

Authors' Note

The authors share equal authorship. Authors' names are in alphabetical order. Eric Jardine is the corresponding author and can be reached at ejardine@vt.edu.

23 Response to Defendant's Motion to Compel, *United States v Michaud* (2015).

Works Cited

Chertoff, Michael. 2017. "A public policy perspective of the Dark Web." *Journal of Cyber Policy* 2 (1): 26–38. doi:10.1080/23738871.2017.1298643.

Chertoff, Michael and Paul Rosenzweig. 2015. *A Primer on Globally Harmonizing Internet Jurisdiction and Regulations*. Global Commission on Internet Governance Paper Series No. 10. Waterloo, ON: CIGI. www.cigionline.org/publications/primer-globally-harmonizing-internet-jurisdiction-and-regulations/.

Chertoff, Michael and Tobby Simon. 2015. *The Impact of the Dark Web on Internet Governance and Cyber Security*. Global Commission on Internet Governance Paper Series No. 6. Waterloo, ON: CIGI. www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security/.

Collier, Ben. 2020. "The power to structure: exploring social worlds of privacy, technology and power in the Tor Project." *Information, Communication & Society* 24 (12): 1728–44. doi:10.1080/1369118X.2020.1732440.

Cox, Joseph. 2016a. "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers." *Vice*, January 6. https://motherboard.vice.com/en_us/article/qkj8vv/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

———. 2016b. "An Admin's Foolish Errors Helped the FBI Unmask Child Porn Site 'Playpen.'" *Vice*, May 16. www.vice.com/en_us/article/nz7e8x/an-admins-foolish-errors-helped-the-fbi-unmask-child-porn-site-playpen.

———. 2016c. "The FBI Hacked Over 8,000 Computers in 120 Countries Based on One Warrant." *Vice*, November 22. https://motherboard.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant.

———. 2017. "DOJ, FBI Executives Approved Running a Child Porn Site." Vice, May 29. https://motherboard.vice.com/en_us/article/bjg9j4/doj-fbi-child-pornography-sting-playpen-court-transcripts.

de Tocqueville, Alexis. 2004. *Democracy in America*. 2 vols. Translated from the French by Arthur Goldhammer. New York, NY: Library of America. First published 1835.

Department of Justice. 2017. "Florida Man Sentenced to Prison for Engaging in Child Exploitation Enterprise." Press Release, May 1. www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise.

Dingledine, Roger, Nick Mathewson and Paul Syverson. 2004. "Tor: The Second-Generation Onion Router." *Proceedings of the 13th Conference on USENIX Security Symposium*, vol. 13, San Diego, CA.

Dolliver, Diana S. 2019. "Emerging Technologies, Law Enforcement Responses, and National Security." *I/S: A Journal of Law and Policy for the Information Society* 15 (1–2): 123–50.

Faizan, Mohd and Raees Ahmad Khan. 2019. "Exploring and analyzing the dark Web: A new alchemy." *First Monday* 24 (5). doi:10.5210/fm.v24i5.9473.

FBI. 2017. "Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay." FBI, July 20. www.fbi.gov/news/stories/alphabay-takedown.

Garcha, Rupinder K. 2018. "NITs a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases." *New York University Law Review* 93 (4): 822–63.

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.

Graham, Roderick and Brian Pitman. 2020. "Freedom in the wilderness: A study of a Darknet space." *Convergence: The International Journal of Research into New Media Technologies* 26 (3): 593–619. doi:10.1177/1354856518806636.

Hennessey, Susan and Nicholas Weaver. 2016. "A Judicial Framework for Evaluating Network Investigative Techniques." *Lawfare* (blog), July 28. www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques#.

Jardine, Eric. 2015. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Global Commission on Internet Governance Paper Series No. 21. Waterloo, ON: CIGI. www.cigionline.org/publications/dark-web-dilemma-tor-anonymity-and-online-policing/.

———. 2018a. "Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies." *New Media & Society* 20 (8): 2824–43. doi:10.1177/1461444817733134.

———. 2018b. "Tor, what is it good for? Political repression and the use of online anonymity-granting technologies." *New Media & Society* 20 (2): 435–52. doi:10.1177/1461444816639976.

———. Forthcoming 2021. "Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention." *American Journal of Criminal Justice*.

Jardine, Eric, Fen Osler Hampson and Dane Rowlands. 2021. "The Political Economy of Good and Evil: Why the Dark Web Still Exists." Unpublished manuscript.

Jardine, Eric, Andrew M. Lindner and Gareth Owenson. 2020. "The potential harms of the Tor anonymity network cluster disproportionately in free countries." *Proceedings of the National Academy of Sciences of the United States of America* 117 (50): 31716–21. doi:10.1073/pnas.2011893117.

Johnson, Aaron, Chris Wacek, Rob Jansen, Micah Sherr and Paul Syverson. 2013. "Users get routed: Traffic correlation on Tor by realistic adversaries." *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*: 337–48.

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

Levine, Yasha. 2014. "Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government." *Pando*, July 16. https://pando.com/2014/07/16/tor-spooks/.

———. 2018. *Surveillance Valley: The Secret Military History of the Internet*. New York, NY: PublicAffairs.

Levy, Leonard W. 1999. "Origins of the Fourth Amendment." *Political Science Quarterly* 114 (1): 79–101. doi:10.2307/2657992.

Liu, Edward C. and Todd Garvey. 2012. "Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act." Congressional Research Service, April 2. https://fas.org/sgp/crs/secrecy/R41742.pdf.

Locke, John. 1796. *Two Treatises of Government: In the Former, The False Principles, and Foundation of Sir Robert Filmer, and His Followers, Are Detected and Overthrown. The Latter Is an Essay Concerning the True Original, Extent, and End of Civil Government*. London, UK: Crowning Educational.

Maréchal, Nathalie. 2018. "Use Signal, Use Tor? The Political Economy of Digital Rights Technology." Ph.D. dissertation, University of Southern California.

Moore, Daniel and Thomas Rid. 2016. "Cryptopolitik and the Darknet." *Survival: Global Politics and Strategy* 58 (1): 7–38. doi:10.1080/00396338.2016.1142085.

Newman, Lily Hay. 2017. "The Feds Would Rather Drop Child Porn Case Than Give Up a Tor Exploit." *Wired*, March 7. www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/.

Norbutas, Lukas. 2018. "Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network." *International Journal of Drug Policy* 56: 92–100. doi:10.1016/j.drugpo.2018.03.016.

Nurmi, Juha and Mikko S. Niemelä. 2017. "Tor De-anonymisation Techniques." *International Conference on Network and System Security*.

Owen, Gareth and Nick Savage. 2015. *The Tor Dark Net*. Global Commission on Internet Governance Paper Series No. 20. Waterloo, ON: CIGI. www.cigionline.org/publications/tor-dark-net/.

Poulsen, Kevin. 2013. "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack. *Wired*, September 13. www.wired.com/2013/09/freedom-hosting-fbi/.

Prince, Matthew. 2016. "The Trouble with Tor." *The Cloudflare Blog*, March 30. https://new.blog.cloudflare.com/the-trouble-with-tor/.

Raymond, Nate. 2015. "Two people in N.Y. charged in massive probe of child porn website." Reuters, July 8. www.reuters.com/article/us-usa-crime-childporn/two-people-in-n-y-charged-in-massive-probe-of-child-porn-website-idUSKCN0PI2CH20150708.

Rose, Janus. 2016. "FBI: Our Malware Sends Unencrypted Evidence, and That's a Good Thing." *Vice*, June 5. www.vice.com/en_us/article/pgkkvv/fbi-our-malware-sends-unencrypted-evidence-and-thats-a-good-thing.

Sartain, J. D. 2013. "Can your IP address give away your identity to hackers, stalkers and cybercrooks?" *Network World*, July 16. www.networkworld.com/article/2168144/can-your-ip-address-give-away-your-identity-to-hackers--stalkers-and-cybercrooks-.html#.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W. W. Norton & Company.

Topor, Lev. 2019. "Dark Hatred: Antisemitism on the Dark Web." *Journal of Contemporary Antisemitism* 2 (2): 25–42.

Weber, Max. 2004. *The Vocation Lectures: "Science as a Vocation" "Politics as a Vocation."* Indianapolis, IN: Hackett Publishing.

Wexler, Rebecca. 2018. "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System." *Stanford Law Review* 70: 1343–1429.

Winter, Philipp. 2017. "Tor upgrades to make anonymous publishing safer." *The Conversation*, March 19. https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641.

Yung, Corey Rayburn. 2016. "F.B.I. Allowed for More Victimization by Permitting a Child Pornography Website." *The New York Times,* January 27. www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/fbi-allowed-for-more-victimization-by-permitting-a-child-pornography-website.

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop It.* New Haven, CT: Yale University Press.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York, NY: PublicAffairs.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline