Florida State University Law Review

Volume 45 | Issue 4 Article 5

Summer 2018

The Race for Privacy: Technological Evolution Outpacing Judicial Interpretations of the Fourth Amendment: Playpen, the Dark Web, and Governmental Hacking

Wade Williams

THE RACE FOR PRIVACY: TECHNOLOGICAL EVOLUTION OUTPACING JUDICIAL INTERPRETATIONS OF THE FOURTH AMENDMENT: PLAYPEN, THE DARK WEB, AND GOVERNMENTAL HACKING

WADE WILLIAMS

I. INTRODUCTION

Despite complying with the new amendments to Federal Rule of Criminal Procedure 41, the Federal Bureau of Investigation's (FBI) broad authorization to remotely access computers at anytime and anywhere within the United States is at odds with the reasonableness and particularity requirements of the Fourth Amendment.

The exponential growth of technology has made life in the twenty-first century something our ancestors would envy, but the idea of allowing the government to perform unknown and undetected searches across the United States, especially in the hidden world of cyberspace, would have our founding fathers turning in their graves. Recognition is owed to the creators of the Constitution—and the Fourth Amendment specifically—for drafting a document that is still living and breathing, because doing so required tremendous vision. Free of British control and in an attempt to eliminate the immediate evils facing our infant country, the drafters of the Bill of Rights sought to prevent history from repeating itself by ratifying ten amendments to the United States Constitution. Their ability to foresee the unforeseeable is unparalleled; however, here in the digital age, the evolution of technology is outpacing the courts' ability to interpret the Fourth Amendment in a manner that can reconcile governmental expedience and efficiency with individual privacy.

This Note will explore the government's use of network investigative techniques to hack unknown computers across the nation, as well as discuss how district courts disagree whether the hacking, albeit based on a warrant, runs afoul of the Fourth Amendment and former Federal Rule of Criminal Procedure 41. For the courts that have found no Fourth Amendment conflict—whether they found that no search and seizure occurred or that an exception applied—their decisions do not comport with existing case law and risk expanding the scope of governmental searches to unimaginable proportions.

Part II will discuss Playpen—the "dark web" child pornographic website that hosted thousands of anonymous users who distributed child pornography.[1] Further, it will discuss the single warrant that was retrieved and ultimately led to thousands of computers being hacked across the globe.

Part III of this Note will consider the jurisdictional requirements that former Rule 41 placed upon warrant-issuing magistrate judges and how the Department of Justice (DOJ) amended them to circumvent jurisdictional restraints. Additionally, Part III will discuss how the new amendments to Rule 41 will only exacerbate the problem of magistrate judges issuing generalized warrants that are covertly exercised.

Part IV delves deep into the Fourth Amendment, expressing its purpose, effect, and protections in light of searches conducted in cyberspace.

1. Ben Dickson, *A Beginner's Guide to the Dark Web*, THE DAILY DOT (July 19, 2018, 2:30 AM), https://www.dailydot.com/layer8/what-is-dark-web/ [https://perma.cc/Z65J-R82D] ("The dark web . . . is . . . a tiny fraction of the web that is only accessible through specialized software such as the Tor browser. However, the term 'dark web' is also often used to refer to the darknet, the overlay networks that are used to anonymize communications and obfuscate both the origin and destination of internet traffic.").

The Fourth Amendment can be interpreted to evolve with our ever-changing technology; however, some courts have been interpreting the Fourth Amendment in a manner that removes the government's hacking from Fourth Amendment constraints, thereby increasing the risk of establishing precedent that would adversely affect the privacy interests of computer owners.

Part V discusses the competing interests courts weigh in deciding whether to suppress evidence. Although one of the ill-favored consequences of suppression is that some factually guilty defendants are released, it might serve as a reminder to the government to respect magistrate judges' substantive and jurisdictional limitations as well as Fourth Amendment rights.

Part VI expresses the damage that a favorable governmental ruling can have on the criminal justice system. Further, it lists alternative routes the government could take to aggressively pursue and ferret out crime without violating constitutional protections or jurisdictional requirements.

II. PLAYPEN AND THE RESULTING WARRANTS

In August 2014, unbeknownst to Google or any visitor to the World Wide Web, a hidden website known as "Playpen" was launched.[2] At first glance, the domain name conjures thoughts of infants' goods and services, and anyone searching for that term would have come across those exact goods. Unfortunately, that impression could not be further from the truth, for this website operated as a forum for discussion and distribution of child pornography.[3] Over the span of just five months, Playpen attracted approximately 158,000 members who contributed to over 95,000 posts and 9,000 topics related to child pornography.[4]

Playpen operated on an anonymous server known as The Onion Router (Tor).[5] The clever name given to the server is symbolic of the way it operates. Much like an onion's multiple layers, Tor receives an individual's internet protocol ("IP") address and embeds

---

2. Government's Opening Brief at Add.57, United States v. Levin, 874 F.3d 316 (1st Cir. 2017) (No. 16-1567), 2016 WL 6600152.

3. *Id.*; Andrew Crocker, *With Remote Hacking, the Government's Particularity Problem Isn't Going Away*, JUST SECURITY (June 2, 2016), https://www.justsecurity.org/31365/remote-hacking-governments-particularity-problem-isnt/ [https://perma.cc/J5TF-8W2J]; Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, WASH. POST: THE VOLOKH CONSPIRACY (Sept. 27, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/?utm_term=.0521b71d06d4 [https://perma.cc/5GTB-7P3D].

4. Government's Opening Brief, *supra* note 2, at Add.57; *see* Crocker, *supra* note 3; *see also* Kerr, *supra* note 3.

5. Government's Opening Brief, *supra* note 2, at 3. For information on Tor, see *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en [https://perma.cc/VQM9-HLTZ].

it deep within layers of identification-concealing measures.[6] Whenever an individual accesses a website, that website reveals the individual's IP address, which contains identifying information about the computer as well as its geographical whereabouts.[7] To prevent this information from being revealed, an individual can download, install, and use Tor.[8] If an individual operating on the Tor network accesses a website, Tor will take the computer's IP address and route it through a virtual circuit of Tor relay computers (otherwise known as "nodes") located around the world.[9] Each node will encrypt the individual's identifying information such that anyone trying to identify the individual will have to decrypt multiple layers.[10] Even if one were to venture through this virtual labyrinth and decrypt the final relay node, it would only reveal what website the communicating information was sent to rather than where it came from, thereby allowing individuals to operate on the internet without revealing their information.[11]

To the same extent that individuals utilize Tor, websites are also able to avail themselves of these identity-concealing methods. Because Playpen is hosted on the Tor network, it operates as a "hidden service" and cannot be located using public lookups or search engines

6. Government's Opening Brief, *supra* note 2, at 3-4; *see Tor: Overview*, *supra* note 5; Online Interview with Carl David Saintilnor, Cyber Security Engineer, ReliaQuest (Mar. 6, 2017); Online Interview with Angel A. Daruna, Graduate Research Assistant in Robotics, Georgia Institute of Technology (Mar. 7, 2017).

7. Government's Opening Brief, *supra* note 2, at 3; Robert Graham, *Some Technical Notes on the PlayPen Case*, ERRATA SECURITY (Sept. 28, 2016), http://blog.erratasec.com/2016/09/some-technical-notes-on-playpen-case.html#.WMHNXYWcFPZ [https://perma.cc/EM93-JSBB]; Kerr, *supra* note 3.

8. Government's Opening Brief, *supra* note 2, at 3; Kim Zetter, *So . . . Now The Government Wants To Hack Cybercrime Victims*, WIRED (May 4, 2016, 7:00 AM), https://www.wired.com/2016/05/now-government-wants-hack-cybercrime-victims/ [https://perma.cc/9TYW-6B3B]; *Tor: Overview*, *supra* note 5; Crocker, *supra* note 3; Kerr, *supra* note 3.

9. Government's Opening Brief, *supra* note 2, at 3-4; Orin Kerr, *Remotely Accessing an IP Address Inside a Target Computer Is a Search*, WASH. POST: THE VOLOKH CONSPIRACY (Oct. 7, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search/?utm_term=.9c1dbe740b61 [https://perma.cc/VR53-SJQ8] (citing United States' Surreply to Defendant's Motion to Suppress at 6-7, United States v. Michaud (W.D. Wash. 2016) (No. 3:15-cr-05351-RJB), 2016 WL 337263); *The Playpen Cases: Frequently Asked Questions, What is Tor?*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whatistor [https://perma.cc/4LS7-GTMV]; *Tor: Overview*, *supra* note 5; Interview with Carl David Saintilnor, *supra* note 6; Interview with Angel A. Daruna, *supra* note 6.

10. *Tor: Overview*, *supra* note 5.

11. Government's Opening Brief, *supra* note 2, at 4; Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Defendant-Appellee at 6, United States v. Levin, 874 F.3d 317 (1st Cir. 2017) (No. 16-1567), 2017 WL 835118; *Tor: Overview*, *supra* note 5; Interview with Angel A. Daruna, *supra* note 6.

such as Google.[12] Unlike websites open to the public, Tor does not communicate through IP addresses but rather through a set of sixteen algorithm-generated characters followed by the ".onion" suffix.[13] Therefore, in order to locate Playpen, an individual must retrieve the unique set of characters from a Playpen member and enter it into the address bar.[14] Ultimately, Playpen's system required prospective members to take multiple steps to hide their identity, such as downloading and using Tor, acquiring the unique Playpen web address, and creating a username distinct from the member's legal name.[15]

A. A Single Warrant to Access Thousands of Computers

On February 20, 2015, FBI Special Agent Douglas Macfarlane submitted an "Affidavit In Support Of Application For Search Warrant" in the United States District Court for the Eastern District of Virginia before Magistrate Judge Theresa Buchanan.[16] According to the affidavit, FBI agents had been monitoring Playpen between September 16, 2014 and February 3, 2015.[17] In December 2014, an unidentified foreign law enforcement agency informed the FBI that Playpen might be operating on a Tor server based out of North Carolina.[18] The FBI corroborated the tip and obtained a warrant in January 2015.[19] The FBI relocated the server to the Eastern District of Virginia and remained dormant while tracking posts and user activity in an effort to build their case so that they would have probable cause to eventually obtain a search warrant to locate the users of Playpen.[20] However, doing so was difficult because, despite revealing the identity and location of the website, the individual members were still operating anonymously on Tor.[21]

This issue led Agent Macfarlane to search for additional investigative techniques, and although other—less intrusive—searches may have been available,[22] Macfarlane's immediate response was to remotely access Playpen members' computers through what is known

12. Government's Opening Brief, *supra* note 2, at 4; *see* Kerr, *supra* note 3.

13. Government's Opening Brief, *supra* note 2, at 4; *Tor: Overview*, *supra* note 5.

14. Government's Opening Brief, *supra* note 2, at 4-5; *see* Kerr, *supra* note 3.

15. Government's Opening Brief, *supra* note 2, at 4-5; Brief for the United States at 3-4, United States v. Workman, 680 F. App'x 699 (10th Cir. 2017) (No. 16-1401), 2016 WL 7536312.

16. Government's Opening Brief, *supra* note 2, at Add.45.

17. *Id.* at Add.57.

18. *Id.* at Add.65.

19. *Id.* at Add.65-66; Graham, *supra* note 7; Kerr, *supra* note 3.

20. *See id.* at Add.66; Brief for the United States, *supra* note 15, at 5.

21. *See* Government's Opening Brief, *supra* note 2, at Add.66.

22. *See infra* Part VI.

as a Network Investigative Technique (NIT).[23] The difference between remote accessing and an NIT is purely semantic. Simply put, remote accessing is "the use of any physical or logical medium to obtain information from a system. This includes, but is not limited to, physical cable connections, passive side channel monitoring, and traditional remote access via networking technologies."[24] Here, the FBI chose the latter of the three; the one many people commonly refer to as "hacking."[25]

On February 20, 2015, after being presented with all the evidence that Agent Macfarlane had available, Magistrate Judge Buchanan signed the infamous "Search and Seizure Warrant" (Warrant) that has been disputed in federal district and circuit courts all over the United States.[26] The Warrant authorized "*any* . . . law enforcement officer" to search computers located in the Eastern District of Virgin-

23. Government's Opening Brief, *supra* note 2, at Add.67-68.

24. Interview with Angel A. Daruna, *supra* note 6.

25. Graham, *supra* note 7; Kerr, *supra* note 3; Crocker, *supra* note 3; *see* Zetter, *supra* note 8; *see also* Mark Rumold, *The Playpen Story: Rule 41 and Global Hacking Warrants*, ELECTRONIC FRONTIER FOUND. (Sep. 26, 2016) [hereinafter *Rule 41*], https://www.eff.org/deeplinks/2016/08/illegal-playpen-story-rule-41-and-global-hacking-warrants [https://perma.cc/YN54-U6EG]. For discussions on the constitutionality of government hacking, see Andrew Crocker, *Why the Warrant to Hack in the Playpen Case Was an Unconstitutional General Warrant*, ELECTRONIC FRONTIER FOUND. (Sep. 28, 2016) [hereinafter *Unconstitutional Warrant*], https://www.eff.org/deeplinks/2016/09/why-warrant-hack-playpen-case-was-unconstitutional-general-warrant [https://perma.cc/6P9F-5QGQ]; Tim Cushing, *Judge Says FBI Can Hack Computers Without a Warrant Because Computer Users Get Hacked All the Time*, TECHDIRT (Jun. 24, 2016, 8:39 AM), https://www.techdirt.com/articles/20160624/05351534808/judge-says-fbi-can-hack-computers-without-warrant-because-computer-users-get-hacked-all-time.shtml [https://perma.cc/L42E-R2PK]; Mark Rumold, *The Playpen Story: Some Fourth Amendment Basics and Law Enforcement Hacking*, ELECTRONIC FRONTIER FOUND. (Sep. 21, 2016) [hereinafter *Hacking*], https://www.eff.org/deeplinks/2016/09/playpen-story-some-fourth-amendment-basics-and-law-enforcement-hacking [https://perma.cc/ZQW3-N775].

26. *Compare* United States v. McLamb, 880 F.3d 685 (4th Cir. 2018), United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), United States v. Levin, 874 F.3d 316 (1st Cir. 2017), United States v. Workman, 863 F.3d 1313 (10th Cir. 2017), United States v. Ammons, No. 16-CR-00011, 2017 WL 4355670 (W.D. Ky. Sept. 29, 2017), United States v. Kahler, 236 F. Supp. 3d 1009 (E.D. Mich. 2017), United States v. Dzwonczyk, No. 15-CR-3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016), United States v. Duncan, No. 15-CR-00414, 2016 WL 7131475 (D. Or. Dec. 6, 2016), United States v. Kienast, No. 16-CR-103, 2016 WL 6683481 (E.D. Wisc. Nov. 14, 2016), United States v. Stepus, No. 15-30028, 2016 WL 6518427 (D. Mass. Oct. 28, 2016), United States v. Johnson, No. 15-00340-01, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016), United States v. Scarbrough, No. 16-CR-035, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016), United States v. Lough, 221 F. Supp. 3d 770 (N.D. W. Va. 2016), United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016), United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va. 2016), United States v. Jean, 207 F. Supp. 3d 920 (W.D. Ark. 2016), United States v. Allain, 213 F. Supp. 3d 236 (D. Mass. 2016), United States v. Anzalone, 221 F. Supp. 3d 189 (D. Mass. 2016), *and* United States v. Broy, 209 F. Supp. 3d 1045 (C.D. Ill. 2016), *with* United States v. Arterbury, No. 15-CR-182, 2016 U.S. Dist. LEXIS 67091 (N.D. Okla. Apr. 25, 2016), United States v. Croghan, 209 F. Supp. 3d 1080 (S.D. Iowa 2016), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), United States v. Levin, 186 F. Supp. 3d (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017), *and* United States v. Workman, 205 F. Supp. 3d 1256 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017).

ia that access Playpen.[27] The Warrant was to be executed at any time of the day on or before March 6, 2015 and could not last for more than two weeks.[28] In addition, officers executing the Warrant were granted the authority to withhold notifying the searched individual for up to thirty days, mainly out of fear that the suspect would destroy all evidence of criminal conduct relating to Playpen.[29] Unfortunately for the FBI, not all Playpen members were located in Virginia. Although prosecutors argued that the search occurred in the Eastern District because the defendants took a "virtual trip" to the Virginia-based website, the FBI installed the NIT on computers outside of the Eastern District of Virginia.[30]

B. Using the NIT to Exercise Dominion and Control over Computers Throughout the Nation

The name alone is the only thing separating an NIT from being considered "hacking."[31] It seems as if the FBI coined this term in an effort to downplay the seriousness of the search and convince the warrant-issuing magistrate that this *technique* is nothing more than a customary investigative practice. However, tech-savvy individuals across the nation understand that the FBI's labeling of this type of search is nothing more than smoke and mirrors.[32] According to Robert Graham, a frequent contributor to a cybersecurity blog called Errata Security, "the name for what the FBI did is 'hacking[,]' and the name for their software is 'malware[,]' not 'NIT[.]' The definitions [do not] change depending upon [who is] doing it and for what purpose. That the FBI uses weasel words to distract from what [it is] doing seems like a violation."[33] Therefore, despite the naming differences, the FBI was able to access Playpen members' computers without their knowledge.[34]

In practice, the NIT remained dormant on Playpen and was activated only when a member logged in with their username and password. At that moment, the malware would be secretly uploaded to the member's

27. Government's Opening Brief, *supra* note 2, at Add.42 (emphasis added).

28. *Id.*

29. *Id.*; Defendant-Appellant's Opening Brief at 75, United States v. Tippens, No. 3:16-cr-05110-RJB-1 (9th Cir. filed Oct. 13, 2017), 2017 WL 6042193.

30. *See* Government's Opening Brief, *supra* note 2, at 30-31; Appellee's Opening Brief at 13, United States v. Levin, No. 16-1567 (1st Cir. filed Oct. 31, 2016), 2017 WL 512509.

31. Graham, *supra* note 7.

32. *Id.*; *see* Orin Kerr, *The Law of Encryption Workarounds*, THE VOLOKH CONSPIRACY (Oct. 14, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/14/the-law-of-encryption-workarounds/?utm_term=.54eb9020240c [https://perma.cc/C5MK-UT7Z]; *Unconstitutional Warrant*, *supra* note 25; *see also* Crocker, *supra* note 3; Zetter, *supra* note 8.

33. Graham, *supra* note 7.

34. *See* Kerr, *supra* note 3.

computer.[35] Once the upload was complete, the malware would prompt the member's computer to send identifying information to a "computer controlled by or known to the government."[36] Such identifying information included, but was not limited to, the member's actual IP address, the media access control (MAC) address, the host's name, the operating system's username, and the type of operating system running on the computer.[37]

Within the two weeks that the FBI operated Playpen, the NIT identified and installed malware on thousands of Playpen members' computers, leading to nearly 130 prosecutions in district courts across the United States.[38] Out of those 130 prosecutions, thirty-seven motions to suppress evidence have been filed, and of those thirty-seven motions only four have resulted in suppression.[39] Furthermore, of those thirty-seven motions to suppress, only four were the product of searches conducted in the Eastern District of Virginia, whereas the other thirty-three prosecutions resulted in searches conducted in nineteen other states.[40]

One of the main concerns held by critics of Magistrate Judge Buchanan's Warrant is that it is too broad—both in terms of places to be searched and things to be seized.[41] Neither the affidavit nor the Warrant contained any reference to specific individuals or computers to be searched.[42] Instead, the Warrant—a virtual adoption of the affidavit—lists the places to be searched as "[t]he activating computers . . . of *any*

35. Government's Opening Brief, *supra* note 2, at 7; Kerr, *supra* note 3; *see generally* Graham, *supra* note 7.

36. Government's Opening Brief, *supra* note 2, at 27-28.

37. *Id.* at Add.44; *Hacking*, *supra* note 25; Graham, *supra* note 7.

38. Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, MOTHERBOARD (July 27, 2016, 12:15 PM), https://motherboard.vice.com/en_us/article/aek4ak/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen [https://perma.cc/YMH7-3SEG]; *see The Playpen Cases: Frequently Asked Questions*, *What Happened in the Playpen Investigation*, ELECTRONIC FRONTIER FOUND., [hereinafter *Playpen Investigation*], https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whathappened [https://perma.cc/QU8B-P8HU]; *see generally* Government's Opening Brief, *supra* note 2, at 17; Brief for the United States, *supra* note 15, at 11; Mark Rumold, *Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation*, ELECTRONIC FRONTIER FOUND. (Sep. 15, 2016), https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation [https://perma.cc/69WQ-JQD2].

39. Brief for the United States, *supra* note 15, at 11; Government's Opening Brief, *supra* note 2, at 19 (citing States v. Croghan, No. 15-CR-48, 2016 WL 4992105 (S.D. Iowa Sep. 19, 2016); United States v. Workman, No. 15-CR-397, 2016 WL 5791209 (D. Colo. Sep. 6, 2016); United States v. Arterbury, No. 15-CR-182 (N.D. Okla. May 12, 2016)).

40. Brief for the United States, *supra* note 15, at 11; *id.* at 12 nn.5-6 (referencing states such as West Virginia.; Wisconsin; North Carolina; Montana; Texas; Arkansas; Nebraska; California; Oregon; Washington; Massachusetts; Ohio; Illinois; Kentucky; South Carolina; Tennessee; Florida; Louisiana; Pennsylvania).

41. *See* Crocker, *supra* note 3; Zetter, *supra* note 8.

42. *See* Government's Opening Brief, *supra* note 2; Crocker, *supra* note 3; *Unconstitutional Warrant*, *supra* note 25.

user or administrator who logs into [Playpen]."[43] Despite the Constitution's intentions otherwise, Magistrate Judge Buchanan's role as the arbiter of probable cause was reduced to nothing more than a rubber stamp on Agent Macfarlane's seemingly self-issued search warrant in an area of expertise with which Judge Buchanan was most likely unfamiliar.[44] As a result of Judge Buchanan's failure to act as a barrier between the FBI and its suspects, this one-size-fits-all Warrant usurped the power of every other federal magistrate in the districts where members' computers were hacked.[45] Judge Buchanan's failure to limit the scope of the Warrant to the Eastern District of Virginia resulted in a direct violation of Federal Rule of Criminal Procedure 41 (Rule 41) every time the FBI installed the NIT on a computer located outside the Eastern District.[46] Just as she had no authority to issue such a geographically-broad warrant, the FBI had no authority to implement the Warrant nor any right to rely upon it. At the time it was issued, Rule 41 was clearly established law and the FBI should have known that its actions were unlawful.[47]

III. RULE 41—THE OLD, THE NEW, AND THE POTENTIAL FOR HARM

In the midst of all of the government hacking, the DOJ was working diligently behind the scenes to amend Rule 41(b).[48] Under the former rule, which governed the Warrant and every subsequent search of Playpen members' computers, a magistrate could not authorize a warrant to search a computer located outside the magistrate's district, even if the location of the computer was unknown to the government.[49] However, instead of forcing the government to comply with the former rule and conduct further investigation to lo-

43. Government's Opening Brief, *supra* note 2, at Add.43 (emphasis added).

44. *See* Tim Cushing, *FBI Deploying Large-Scale Hacking with Little to No Judicial Oversight*, TECHDIRT.COM (Jan. 7 2016, 11:42 AM), https://www.techdirt.com/articles/20160107/06414333264/fbi-deploying-large-scale-hacking-with-little-to-no-judicial-oversight.shtml, *and* Joseph Cox, *Judge in FBI Hacking Case Is Unclear on How FBI Hacking Works*, MOTHERBOARD (Jan. 27, 2016 12:50 PM), https://motherboard.vice.com/en_us/article/4xave3/judge-in-fbi-hacking-case-is-unclear-on-how-fbi-hacking-works (discussing Magistrate Judge Buchanan's unwillingness to comment on her understanding of how the NIT operates); Zetter, *supra* note 8.

45. *See* Crocker, *supra* note 3.

46. *Id.*; *Unconstitutional Warrant*, *supra* note 25.

47. *Rule 41*, *supra* note 25; *see* Government's Opening Brief, *supra* note 2, at 21; *see generally* Kerr, *supra* note 3.

48. *See* ADVISORY COMMITTEE ON CRIMINAL RULES 155-58 (Apr. 7-8, 2014) http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf.

49. Brief for the United States, *supra* note 15, at 9-10.

cate the suspects' computers, the DOJ intended to bypass the former requirement through amendment.[50]

A. Without Authorization Under Former Federal Rules of Criminal Procedure 41(b) the Warrant Was Void Ab Initio

Many prosecutors have argued, in both district and circuit courts, that Rule 41(b) authorized Judge Buchanan to issue the Warrant; and even if it did not, any violation of the rule does not warrant suppression because the FBI did not act in bad faith and no prejudice resulted from the Warrant.[51] However, even if the government were to successfully argue against a finding of prejudice or bad faith, those arguments operate on the faulty presumption that there was a valid warrant at the outset. Under the facts of Playpen, if the government concedes that Judge Buchanan lacked authority under Rule 41 to issue the Warrant, then they cannot reserve the argument that suppression is unavailable due to the absence of bad faith or prejudice because without authority to issue the Warrant under Rule 41, the Warrant was void *ab initio*.

First, Judge Buchanan never had the authority to grant the exercise of the Warrant outside the Eastern District of Virginia because Rule 41(b)—at the time the Warrant was issued—did not allow magistrates to issue warrants that would extend outside of the district in which they resided.[52] Despite the clear and plain language of former Rule 41(b), the government argued for a more purposeful interpretation of the rule in order to broaden the scope of Judge Buchanan's authority.[53] In *United States v. Lemus*, the government relied upon the Supreme Court decision in *United States v. New York Telephone Co.*, which held that a twenty-day pen register warrant complied with (former) Rule 41 despite the ten-day limit for a

50. *See* ADVISORY COMMITTEE, *supra* note 48, at 155-57.

51. *See, e.g.*, Government's Opening Brief, *supra* note 2, at 43-44 (arguing that no prejudice occurred from the alleged Rule 41(b) error); United States' Surreply to Defendant's Motion to Suppress at 2, United States v. Michaud, No. CR15-5351RJB (W.D. Wash. filed Dec. 21, 2015), 2016 WL 337263 (arguing that even if use of the NIT violated Rule 41, suppression is unwarranted where defendant cannot establish prejudice or bad faith); Government's Opposition to Defendant's Motion to Suppress Evidence at 7-8, United States v. Lemus, No. SACR 15-137-CJC (C.D. Cal. Aug. 8, 2016), 2016 WL 4208436 ("[T]he NIT Warrant did not violate Rule 41, and if it did, suppression is not the appropriate remedy as the . . . defendant suffered no prejudice, and the NIT Warrant was executed in good faith . . . ."), *available at* https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2016/10/Acevedo-Lemus-Brief.pdf.

52. *See* ADVISORY COMMITTEE, *supra* note 48, at 156 n.2 ("[A] magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district[.]" (quoting former Rule 41(b)(1))).

53. Government's Opposition to Defendant's Motion to Suppress Evidence, *supra* note 51, at 19.

search.[54] The Court reasoned that Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause" and that the flexible reading was supported by Rule 57(b), which allowed a court to proceed in any lawful manner that is not inconsistent with the rules or any applicable statute if no procedure were specifically prescribed by the rule.[55]

Nevertheless, while a broad interpretation of Rule 41 may be appropriate in some cases, it is not so here. The government's reliance upon this outdated case to support a broad reading of Rule 41 is inappropriate because *New York Telephone Co.* is hardly analogous to the facts presented here. The only commonality between the two is that the government used technology to try to locate an individual. Other than that, the two cases remain in stark contrast to one another. In *New York Telephone Co.*, the issue was whether Rule 41 allowed for a ten-day extension in the search for one individual's telephone in a location known to be within the judge's district, whereas the issue with Playpen was whether Rule 41 allowed the search of 8,000 computers belonging to unknown individuals in unknown locations across 120 countries.[56] In essence, the government was asking Rule 41 to be read broadly enough to allow one magistrate to issue a warrant that would allow the FBI to hack unknown individuals in unknown locations even if the location was halfway across the world.

Furthermore, other Federal Rules of Criminal Procedure are unable to broaden former Rule 41's scope of authority. Rule 57(b), relied upon in *New York Telephone Co.* and *Lemus*, is inapplicable here because former Rule 41(b) specifically prescribed that the magistrates had authority "to issue a warrant to search for and seize a person or property located *within the district*."[57] Whether considering the letter of the law or the spirit of the law, it is unmistakable that Judge Buchanan was authorized to issue warrants only for searches conducted in her district. If the purpose or text of the rule had indicated otherwise, the DOJ would not have sought an amendment allowing a judge to issue a warrant that could be executed outside of her district. Similarly, the government's opening brief in *United States v. Levin* relied upon *New York Telephone Co.* to read Rule 41(b) broadly so that the NIT fell under the definition of "tracking device" in Rule 41(b)(4).[58] If the NIT were to be classified as a tracking device, Rule

54. United States v. New York Tel. Co., 434 U.S. 159 (1977).

55. Government's Opposition to Defendant's Motion to Suppress Evidence, *supra* note 51, at 19 (quoting *N.Y. Tel. Co.*, 434 U.S. at 169-70).

56. *Id.*; C. Aliens, *The FBI Hacked 8,000 Computers in 120 Countries with a Single Warrant*, DEEP DOT WEB (Dec. 1, 2016), https://www.deepdotweb.com/2016/12/01/fbi-hacked-8000-computers-120-countries-single-warrant/ [https://perma.cc/YS7H-S3TR].

57. FED. R. CRIM. P. 41(b)(1) (emphasis added).

58. Government's Opening Brief, *supra* note 2, at 24-25.

41(b)(4) would have authorized the Warrant to be executed outside of Judge Buchanan's district. But again, this was another attempt by the government to retroactively validate an invalid warrant. Agent Macfarlane's "Affidavit In Support Of Application For Search Warrant" never referred to the NIT as a tracking device or method for tracking individuals, and the NIT does not function like a tracking device.[59] The NIT serves to locate an individual identified with a particular computer, but it cannot track an individual's or a computer's movements.[60]

A warrant that is issued and executed beyond a magistrate's territorial jurisdiction is void *ab initio*.[61] A warrant that is void *ab initio* ("[n]ull from the beginning")[62] has the same legal effect as no warrant at all. Because Judge Buchanan issued a warrant that authorized execution beyond the Eastern District of Virginia, the FBI was essentially operating without a warrant for every use of the NIT on computers located outside that district. Therefore, the FBI conducted warrantless searches of computers located outside the Eastern District of Virginia.

A judge acts outside the law when issuing a warrant without any authority, thus the warrant is void rather than simply voidable.[63] This is precisely why the government's supplemental arguments for lack of prejudice and bad faith are meritless. Those arguments come into play only when a warrant is voidable, such as with judicial error.[64] Similarly, the good faith exception to the exclusionary rule applies to subsequently invalidated warrants (like lack of probable cause), not warrants that are void upon their inception, such as the one here.[65]

B. *DOJ Taking the Easy Way Out: Fixing What is Not Broken for the Sake of Convenience*

Prompted in part by a Southern District of Texas decision to deny a warrant to remotely access a computer in an unknown location on April 2013, the DOJ formally requested an amendment to Rule 41 in April 2014 to circumvent future decisions such as these.[66] Unsatisfied with the limited ability of magistrates to issue warrants that can only be executed in the district where they reside, the Acting Attorney General sent a letter to the Advisory Committee on Criminal Rules (Advisory Committee) in September 2013 requesting that a magis-

59. Appellee's Opening Brief, *supra* note 30, at 12.

60. *Id.*

61. United States v. Workman, 205 F. Supp. 3d 1256, 1266-67 (D. Colo. 2016).

62. *Id.* at 1267; *Void*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining ab initio).

63. *Workman*, 205 F. Supp. 3d at 1267.

64. *See id.*

65. *See id.*

66. Appellee's Opening Brief, *supra* note 30, at 2 (citing *In re* Warrant to Search a Target Computer at Premises Unknown, 758 F. Supp. 2d 753 (S.D. Tex. 2013)); *id.* at 2 n.2.

trate's authority to issue a warrant be expanded when the location of the suspect's computer is unknown.[67] Then, the chair of the Advisory Committee, Judge Reena Raggi of the United States Court of Appeals for the Second Circuit, requested that the DOJ provide potential search warrants that would be authorized under the new rule to a subcommittee, which would examine any issues that would arise from the new rule.[68] Despite the issues brought to light by the subcommittee, the amendments were submitted to the Supreme Court, adopted, and submitted to Congress on April 28, 2016.[69] The amendments took effect on December 1, 2016 (largely due to a lame-duck administration that was unwilling to challenge them).[70] Among the issues observed by the subcommittee, the most notable concerned forum shopping, particularity,[71] and lack of notice.[72]

1. *The Current Rule's Lack of Specificity and Jurisdictional Restraints Will Induce Forum Shopping*

The new amendments to Rule 41 have increased the potential for abuse in obtaining warrants. Although the new rule will expedite the warrant-obtaining process, federal agents will be more inclined to seek warrants from FBI-friendly magistrates. Therefore, if a magistrate in a district where criminal activity may have taken place is unlikely to issue a search warrant, an agent can seek a warrant from a magistrate in the neighboring district and eventually implement it in the district where the former magistrate would have denied the warrant. Interestingly enough, the magistrate who initially denied granting a search warrant for his district will have no authority to prevent the same FBI agent from exercising the warrant and conducting a search in his district.

This concern was present and known to the Advisory Committee before the new rule was adopted; however, they chose to ignore the arguments of those who opposed the amendments.[73] For example, one critic, "Orin Kerr, a former federal cybercrimes prosecutor who is on the judicial rules committee that evaluated the proposed amendments, has ex-

67. *Id.* at 2; ADVISORY COMMITTEE, *supra* note 48, at 155.

68. ADVISORY COMMITTEE, *supra* note 48, at 155-59.

69. *See* Letter from John G. Roberts, Chief Justice of the U.S. Supreme Court, to Paul D. Ryan, Speaker of the House of Representatives & Joseph R. Biden, Jr., President, United States Senate (Apr. 28, 2016) [hereinafter Letter from John G. Roberts], *available at* http://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.

70. FED. R. CRIM. P. 41(b)(1); *see also* Zetter, *supra* note 8.

71. *See infra* Section IV.C (further discussing particularity as it relates to the Fourth Amendment).

72. ADVISORY COMMITTEE, *supra* note 48, at 159.

73. *See* ADVISORY COMMITTEE, *supra* note 48, at 158-61.

pressed concern that letting a single magistrate issue one warrant for multiple searches would facilitate 'forum shopping.'"[74]

2. *Lack of Notice*

In the physical realm, an individual is immediately put on notice when the individual's house or property is searched. This informs the individual that she has now become the subject of an investigation and that the government has interests adverse to her, thereby allowing the individual time to prepare an adequate defense. However, for a search conducted in cyberspace, such as remote accessing, the individual being searched is unaware that a search is being conducted or that the individual is the subject of an investigation. For the simple fact that the individual happened to be searched electronically, she is at a disadvantage because of the failure to be notified of the search at the time it occurred.

Under the new Federal Rules of Criminal Procedure 41(f)(1)(C),

> [t]he officer executing . . . a warrant to use remote access to search electronic storage media and seize or copy electronically stored information . . . must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.[75]

Although it appears as if those searched via remote access will be provided adequate notice, the committee note to this rule makes it clear that notice can be delayed pursuant to Rule 41(f)(3) in "limited circumstances."[76] Yet, if the government's behavior is any indication of the type of notice that searched individuals are to receive, it appears as if all types of activity will fall under the "limited circumstances" umbrella such that the government can delay notifying searched individuals. Indeed, here the FBI sought and received a delay in the NIT Warrant even before Rule 41 was amended.[77] Consequently, this new rule has great potential for abuse because the costs seriously outweigh the benefits. At best, deferring to delayed notice prevents a few suspects from destroying evidence before apprehension. At worst, the government prevents those with no motive to destroy evidence or evade arrest from preparing a proper defense.

Furthermore, the language of Rule 41(f)(1)(C) is vague and unhelpful, especially in contexts such as these where the suspect's iden-

74. Zetter, *supra* note 8.

75. FED. R. CRIM. P. 41(f)(1)(C).

76. *Id.* advisory committee's note to 2016 amendment.

77. Government's Opening Brief, *supra* note 2, at Add.41.

tification and location are unknown. Language such as use "reasonable efforts" to leave notice "where the officer took the property" is unavailing to officers trying to serve unknown individuals in unknown locations.[78] Ambiguity aside, even if the officers are able to notify the searched individual via electronic means, there is no telling whether electronic notification is adequate enough to inform the individual that a search has occurred. There is a concern that electronic notification, such as pop-up or splash pages, could appear like a phishing attack and risk being ignored.[79] In addition, if the government begins to heavily rely on this type of notice, "enterprising hackers" could mimic this form of notice and use it as a tactic to trick people into clicking on virus-filled attachments.[80]

C. The New Amendments to the Federal Rules of Criminal Procedure 41 Are Not Purely Procedural, but Rather Substantive with Fourth Amendment Implications

In their request to amend Federal Rule of Criminal Procedure 41, the DOJ sought approval from the Supreme Court to make changes to the rule which appeared procedural on their face but were substantive in effect.[81] Federal courts can make rule changes as long as they are solely procedural;[82] however, the amendments here are substantive because they determine who can be searched, when they can be searched, and how they can be searched. Only Congress has the power to implement substantive changes to rules, and in an attempt to circumvent congressional requirements, the DOJ masked their substantive changes in procedural terms.[83]

Critics of the newly amended rules request that Congress enact a specific statute which would regulate the use of governmental hacking, just as they have in the past with technologies such as wiretapping.[84] According to Peter Goldberger, a member of the National Association of Criminal Defense Lawyers, "[t]he accessing of thousands of computers by the government . . . should be the subject of a statute passed by Congress—not a short simple procedural rule, but a com-

---

78. *See* FED. R. CRIM. P. 41(f)(1)(C).

79. Zetter, *supra* note 8.

80. *Id.*

81. *See* Letter from John G. Roberts, *supra* note 69.

82. *See* Zetter, *supra* note 8; *see also* Jennifer Daskal, *Rule 41 Has Been Updated: What's Needed Next*, JUST SECURITY (Dec. 5, 2016), https://www.justsecurity.org/35136/rule-41-updated-needed/ [https://perma.cc/Q9AU-RSYA].

83. Crocker, *supra* note 3; Zetter, *supra* note 8. *Compare* Daskal, *supra* note 82, *with* Susan Hennessey, *Rule 41: Resolving Procedural Debates to Face the Tough Questions on Government Hacking*, LAWFARE (Dec. 1, 2016, 2:38 PM), https://www.lawfareblog.com/rule-41-resolving-procedural-debates-face-tough-questions-government-hacking [https://perma.cc/6QZK-FL5V].

84. Zetter, *supra* note 8.

plex multi-provisioned statute."[85] Goldberger goes on further to say that the "statute [should state] who is allowed to do this, when they are allowed to do it, what justifies doing it, to whom it can be done and the procedures for doing it."[86] Unfortunately, the changes have only been in effect since December 1, 2016, and it seems unlikely that any changes will come because not enough time has passed for courts and legislatures to gauge the effectiveness of the amendments.

IV. EXPANSION OF GOVERNMENTAL SEARCHES RISKING THE EXTINCTION OF FOURTH AMENDMENT PROTECTIONS

There is a common understanding in the legal community that bad facts breed bad law. The facts surrounding the Playpen investigation are horrid and unspeakable, but despite the illegal and immoral activity taking place, the FBI must conduct their investigation within constitutional bounds even if it would limit the FBI's ability to locate and apprehend suspects and risk allowing those engaged in criminal activity to escape arrest. However, this does not mean that the FBI is without a constitutional investigative alternative.[87]

Here, the facts prompted the FBI to operate in a manner that has produced controversy amongst district courts on whether evidence obtained as a result of the NIT should be suppressed. Although a procedural violation may not warrant suppression of evidence, a constitutional violation often will.[88] Fortunately, most of the cases arising from the Playpen Warrant have been decided at the district court level; however, there are now a few circuit courts hearing issues related to the Warrant on appeal.[89] While the district court decisions do not establish precedent, the risk of limiting Fourth Amendment protections is heightened because the circuit court decisions, as well as any subsequent Supreme Court decisions, will be binding upon the government and other courts.[90] These decisions will create lasting legal rules that could allow the government to secretly access and search a location that can hold more personal and private infor-

---

85. *Id.*

86. *Id.*

87. *See infra* Part VI.

88. United States v. Krueger, 809 F.3d 1109, 1113-14 (10th Cir. 2015); Kerr, *supra* note 3.

89. Orin Kerr, *What's Missing in the Government's Briefs in the Playpen Warrant Cases*, WASH. POST: THE VOLOKH CONSPIRACY (Feb. 20, 2017) [hereinafter *What's Missing*], https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/20/whats-missing-in-the-governments-briefs-in-the-playpen-warrant-cases/?utm_term=.677a4e2b0e48 [https://perma.cc/8CMT-XQQB] (citing United States v. Workman, United States v. Horton, and United States v. Levin).

90. *Hacking*, *supra* note 25.

mation than what is considered the apex of Fourth Amendment Protection—the home.[91]

A. Harking Back to the Framers' Concerns

The Fourth Amendment can be divided into two clauses: the reasonableness clause and the warrant clause; however, this Note focuses on the latter.[92] The Fourth Amendment protects citizens and their effects from unreasonable searches and seizures by ensuring that "no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[93] In drafting the Fourth Amendment, the framers of the Constitution were concerned with the issuance of writs of assistance, modernly known as general warrants, which granted British officers the authority to search any house for contraband without having to specify which house or person was the subject of the search.[94] James Otis, a former English advocate-general, who refused to defend the legality of general warrants, stated that writs of assistance are "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law-book. . . . It is a power that places the liberty of every man in the hands of every petty officer."[95] Two and a half centuries later, it seems as if we are returning to the very evil the framers of the Constitution sought to destroy by drafting the warrant clause out of the Fourth Amendment. Our founding fathers—and even modern-day judges—would never issue a warrant to search multiple homes on one street, let alone a warrant to search an unlimited number of unknown individuals in unknown locations. To be sure, for the installation of the NIT on unknown computers to be considered a search, individuals must have a reasonable expectation of privacy in those computers.

The warrant clause is triggered only when the government's conduct is classified as a search or seizure.[96] For Fourth Amend-

91. Wayne A. Logan, Gary & Sallyn Pajcic Professor, Fla. State Univ. Coll. of Law, Lecture on "Criminal Procedure, Police" (Fall 2016) (notes on file with the author) (citing Welsh v. Wisconsin 466 U.S. 2091 (1984)).

92. *NCJRS Abstract*, NAT. CRIM. JUST. REFERENCE SERV., ncjrs.gov/App/Publications/abstractt.aspx?ID=122962 [https://perma.cc/KV3E-2ULJ]. Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 AM. CRIM. L. REV. 1389, 1389 (1989).

93. U.S. CONST. amend. IV.

94. Encyclopedia Britannica, *Writ of Assistance*, BRITANNICA.COM, https://www.britannica.com/topic/writ-of-assistance [https://perma.cc/EG5H-23G9].

95. James Otis, *Against Writs of Assistance*, NAT'L HUMAN. INSTIT., http://www.nhinet.org/ccs/docs/writs.htm [https://perma.cc/4MYR-F3VX].

96. Barry Jeffrey Stern, *Warrants Without Probable Cause*, 59 BROOK. L. REV. 1385, 1415, 1427 (1994) (discussing the interpretation of a warrant requirement regardless of probable cause).

ment purposes, a *search* occurs when a state actor (such as an FBI agent) intrudes upon a person's reasonable expectation of privacy, which, under *Katz v. United States*, is established when a person expresses a subjective manifestation of privacy that society is prepared to recognize as reasonable—what is referred to as objective manifestation.[97] While the subjective manifestation prong is easily established once a person takes affirmative steps to protect their privacy interests, the objective manifestation prong is harder to establish because it is what a modern society would recognize as objectively reasonable. This standard, when viewed through the eyes of the court—which, more often than not, is comprised of older judges and magistrates who are unfamiliar with the modern technology used by the government to search and investigate individuals—can result in shaky outcomes.[98]

Once it has been established that a person has a reasonable expectation of privacy over their person, house, papers, or effects, any interference with that expectation of privacy by a state actor will constitute a search under the Fourth Amendment.[99] Thus, a warrant is required before any search can begin; yet, contrary to popular belief, a warrant alone does not satisfy the Fourth Amendment's warrant clause.[100] Under that clause, the warrant must satisfy the particularity requirement by specifically "describing the place to be searched, and the persons or things to be seized."[101] Again, the framers were concerned with generalized warrants; thus, in implementing the particularity requirement, they did so with three purposes in mind.[102]

First, personalized knowledge as to the specifics of an alleged crime is a prerequisite to a constitutionally-valid search.[103] The officers must know *who* they are searching and *where* they are searching. Next, requiring the warrant to contain reasonable particularity operates as an ex ante commitment on the state actors.[104] This prevents officers, in situations such as this one, from supporting a facially-

97. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (providing the two-prong approach to a reasonable expectation of privacy).

98. Wayne A. Logan, Gary & Sallyn Pajcic Professor, Fla. State Univ. Coll. of Law, Lecture on "Criminal Procedure, Police" (Fall 2016) (notes on file with the author) (citing Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) and discussing the hardships senior magistrate judges face in deciding questions of reasonable expectations of privacy with respect to evolving technology).

99. *Id.*

100. *Id.*

101. U.S. CONST. amend. IV.

102. Wayne A. Logan, Gary & Sallyn Pajcic Professor, Fla. State Univ. Coll. of Law, Lecture on "Criminal Procedure, Police" (Fall 2016) (notes on file with the author).

103. *Id.*

104. *Id.*

insufficient warrant with after-the-fact probable cause solely because they happened to apprehend someone engaged in the type of criminal act that was described in the affidavit in support for a warrant. Lastly, and most importantly, the particularity requirement prevents the issuance of blank check warrants.[105] This purpose grew directly out of the framers' fear of generalized warrants, and it prevents officers from searching multiple houses, or anywhere within a house, without specifying exactly what it is they are searching for.

When reviewing search warrants, courts will view the warrant in light of these three purposes and look at what the officers knew or should have known in determining whether the warrant reasonably and sufficiently describes the people or places to be searched.[106] If a court determines that the warrant lacks particularity, any evidence obtained as a result of the execution of that warrant will be suppressed.[107] However, if an officer later determines that the particularity requirement is not satisfied, the officer can rehabilitate the warrant and prevent evidence from being suppressed at trial by exercising due diligence—a simple call to the warrant-issuing magistrate to inform her of any new information would suffice.[108]

B. Setting the Stage for a Warrant: [Un]Reasonable Expectations of Privacy and Assessing Searches in Cyberspace

In what is considered "the most extensive use of government malware by a U.S. law enforcement agency in a domestic criminal investigation,"[109] district courts across the nation have struggled to maintain consistency as to whether the fruits obtained from searches conducted on the basis of the Warrant should be suppressed.[110] Of the district courts that have denied suppression, a majority of them have held that suppression is improper because an exception to the exclusionary rule applies, whereas a minority of courts have held that evidence should not be suppressed because Playpen members had no reasonable expectation of privacy in their computers or IP addresses.[111] Although a minority of district courts have held that the FBI

105. *Id.*

106. *Id.*

107. *Id.*

108. *Id.*

109. *Playpen Investigation*, *supra* note 38.

110. Kerr, *supra* note 3.

111. Government's Opening Brief, *supra* note 2, at 17-19. *See* United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016) (finding that a warrant was not required because the defendant had no subjective expectation of privacy in his IP address); United States v. Allain, 213 F. Supp. 3d 236, 246 n.5 (D. Mass. 2016) (finding that the FBI did not require a warrant to discover the IP addresses of Playpen users because there is no reasonable expectation of privacy in an IP address); United

did not "search" Playpen members' computers, arguments that the FBI's actions did not constitute a "search" have not been popular in governmental appellate briefs.[112] It appears as if the government has abandoned that argument and instead focused its attention on disputing the absence of particularity in the Warrant with respect to who and where it gives authority to search.[113] Nevertheless, it is worth noting why some courts have found that no search occurred, on what basis they made that determination, and why most courts have classified the FBI's use of the NIT as a search despite finding that Playpen members had no reasonable expectation of privacy in their IP addresses.

1. The Third-Party Doctrine and Privacy Interests in IP Addresses

The fact that some courts are unwilling to recognize that Playpen members have a reasonable expectation of privacy in their IP addresses demonstrates that the judiciary may be somewhat out of touch with reality. Indeed, the sole purpose of using Tor to conceal IP addresses is to maintain privacy. There is an argument to be made that Playpen members have a reasonable expectation of privacy in their IP addresses because they manifest a subjective expectation of privacy by using Tor to conceal those addresses. However, as many courts have correctly pointed out, there can be no reasonable expectation of privacy in those IP addresses because the use of Tor prohibits the members from satisfying the objective manifestation prong.[114] By using Tor, Playpen members are transferring their IP addresses through relay computers around the world.[115] According to the third-party doctrine, because each relay computer belongs to a third party, members utilizing Tor do not have a reasonable expectation of privacy in information they knowingly and voluntarily disclose to third parties.[116] Nevertheless, the fact that Playpen members do not have a reasonable expectation of privacy in their IP addresses does not grant the FBI the authority to obtain them in the manner in which they did, for the Fourth Amendment protects the

States v. Werdene, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016) (holding that the defendant did not have a reasonable expectation of privacy in his IP address, and thus, the NIT used by the government could not be considered a "search" under the Fourth Amendment).

112. *See What's Missing*, *supra* note 89 (citing government's briefs in United States v. Workman, United States v. Horton, and United States v. Levin).

113. *See id.*

114. *See Acevedo-Lemus*, 2016 WL 4208436, at *4; *Allain*, 213 F. Supp. 3d at 246 n.5; *Werdene*, 188 F. Supp. 3d at 444.

115. *Tor: Overview*, *supra* note 5.

116. *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 568 (2009).

manner in which the information was received just as much as it protects the information itself.[117]

District courts basing denial of suppression on the third-party doctrine have misapplied the doctrine to the facts surrounding the Playpen searches. An example revealing the proper and improper use of the third-party doctrine can be found through the polarized applications of the doctrine in *United States v. Horton*[118] and *United States v. Werdene*,[119] with the former being the proper and the latter being the improper. *Werdene* is one of multiple court decisions that relied upon the third-party doctrine, and although it may be true that Playpen members had no reasonable expectation of privacy in their IP addresses, decisions such as *Werdene* fail to realize what the court in *Horton* found: the FBI did not obtain the IP addresses from a third party (or more specifically, the Tor relay computers).[120] The FBI is unable to avail themselves of the benefits of the third-party doctrine for information volunteered to third parties unless they receive that information from the third party itself. As illustrated by Orin Kerr,

> If the [FBI] want to read today's newspaper, they can't break into my house and open my desk drawer to find my copy without committing a search. The fact that they could have read the newspaper by finding a copy in public doesn't mean they can break into my house to read mine.[121]

Therefore, if the FBI wanted to rely upon the third-party doctrine they should have received the IP addresses from Tor. Instead, the government attempted to—and in some cases successfully did—use the third-party doctrine as a tool for distraction to divert courts from the fact that the FBI's NIT compelled Playpen members' computers to transmit their IP addresses and other identifying information to the FBI's servers located in Virginia. The sole reason the FBI utilized the NIT is because they could not retrieve identifying information from Tor.[122] Consequently, under the facts of the Playpen cases, there is either the use of the NIT on Playpen members' computers or the proper use of the third-party doctrine; the two cannot coexist with the way the FBI conducted the investigation.

---

117. Kerr, *supra* note 3; United States v. Workman, 205 F. Supp. 3d 1256, 1264-65 (D. Colo. 2016).

118. 863 F.3d 1041, 1046-47 (8th Cir. 2017).

119. 188 F. Supp. 3d 431, 445 (E.D. Pa. 2016).

120. *Horton*, 863 F.3d at 1046-47.

121. Kerr, *supra* note 9.

122. *See* Government's Opening Brief, *supra* note 2, at Add.55-57.

2. Pushing the Envelope: Limiting the Privacy Interests in Computers

While courts differ on the specifics of the NIT and where to draw the line between what does and does not constitute a search, one court has gone so far as to hold that Playpen members can never have a reasonable expectation of privacy in their computers because hacking is commonplace in the digital world.[123] According to Judge Morgan Jr. in *United States v. Matish*, "the deployment of the NIT to capture identifying information found on [the] [d]efendant's computer does not represent a search under the Fourth Amendment, and no warrant was needed."[124] In finding that no search had occurred, Judge Morgan Jr. improperly equated an expectation of security with an expectation of privacy to draw the conclusion that no privacy expectations exist in Playpen members' computers.[125] Unfortunately, this reasoning defies logic and reality, and it would virtually extinguish Fourth Amendment protections in any scenario in which a person could hypothetically breach another individual's security interest. For example, a person would have no expectation of privacy in a locked chest inside a locked room of a locked house *if* another person could break into that house, enter the room, and pick the lock on the chest. While that example is the logical outcome of Judge Morgan Jr.'s holding, he instead analogizes the hacking of computers to police officers peering through open blinds on a window to see what is inside a house.[126] However, Judge Morgan Jr., in his hypothetical, failed to recognize that the officer engaged in legal activity by peering through the blinds; the same cannot be said for those who hack computers. Interestingly, the judge's reasoning is further strained by the fact that, in his hypothetical, the security of the home is not placed in jeopardy. The officer did not risk breaching the home's security, but rather observed a small portion of the interior of the home from a legal vantage point. While it may be difficult to analogize cyberspace activity with activity in the physical realm, Judge Morgan Jr. clearly misses the mark here with his analogy. His widespread-hacking rationale and incongruent peeping-cop explanation lead to two results that do not comport with existing case law: Playpen members have no reasonable expectation of privacy in their computers because 1)

123. *Compare* United States v. Matish, 193 F. Supp. 3d 585, 619 (E.D. Va. 2016) (arguing that the mere possibility of computer hacking removes an expectation of privacy over the computer), *with* California v. Greenwood, 486 U.S. 1625, 1636 (1988) (Brennan, J., dissenting) (arguing that the mere possibility of a burglary does not negate an expectation of privacy in the home).

124. *See Matish*, 193 F. Supp. 3d. at 620.

125. *See id.* at 618-19.

126. *Id.* at 620.

someone could breach the members' security by illegally hacking the computer; or 2) someone could perform the digital equivalent of peering through blinds. The first result encourages police to act illegally because the public *can*, while the second result does not apply here because Playpen members masked their identity and location through Tor.

Similar to the issue presented in *Matish*, the Court in *Florida v. Riley*[127] was tasked with determining whether a search had occurred when officers flew over the defendant's house in a helicopter to look into his fenced backyard. The Court held that if information is made available to the public, then an officer can act as any member of the public could and obtain the information free from Fourth Amendment restrictions.[128] In holding that a search had not occurred, the majority focused on the fact that the officers had hovered over the defendant's yard at an altitude that was legally permissible, and because any member of the public could theoretically hover over the defendant's yard at that altitude, the officers' conduct did not rise to the level of a search.[129] Although Judge Morgan Jr. followed the *could* rationale of *Riley*, he did so improperly. In determining whether police behavior is considered a search, the question is not whether any member of the public could obtain the information, but whether the officer acted as any member of the public could *in obtaining* public information. Therefore, if a member of the public acts illegally in obtaining private information, an officer cannot act similarly because the public was not permitted to act in such a manner. Here, the FBI's use of the NIT is a search for two reasons: 1) the information sought, while normally publically accessible, was concealed through Tor and not available to the public; and 2) the public could not access the information without acting illegally by hacking Playpen members' computers.

C. *The Deal Breaker: The Warrant and its Lack of Particularity in Light of the Length and Results of the Investigation*

It is worth noting the incongruence between existing case law and the district courts' failure to find a search. The issue here, however, does not pertain solely to whether Playpen members had a reasonable expectation of privacy in their computers or IP addresses; the additional question is whether the FBI's use of the NIT was considered a search. It is now apparent that the privacy interests existed, and the subsequent search occurred. Ultimately, the main issue of

127. 488 U.S. 693, 696 (1989).

128. *Id.*

129. *Id.* at 697.

whether suppression of evidence was warranted depends upon the particularity—or lack thereof—of the FBI's search warrant. Thus, because the law deems computers as deserving of Fourth Amendment protection, it demands that the FBI limit the scope of its intrusion by describing to the magistrate, as particularly as possible, where they will search, who they will search, and how they will search.

Here, the FBI allowed Playpen to operate for two weeks while they tracked Playpen members and obtained certain identifying information about them. Since the FBI ran Playpen for two weeks after assuming control of the server, they should have been able to provide individual-specific information to Judge Buchanan, such as a member's username, number of log-ins, and material downloaded and distributed. However, instead of tailoring their request for a warrant to specific members, the FBI sought a blanket-search warrant by requesting authority to hack any computer that appeared to belong to a member who logged in to Playpen. If that were the FBI's intention, they could have obtained relatively similar information by hosting Playpen for a week at most, instead of allowing Playpen—a child pornographic website—to remain operational for an additional two weeks. For engaging in what some would consider to be an unethical investigative technique, one would expect the FBI to have had the opportunity to provide more individual-specific information in their request for a search warrant.

V. A BATTLE OF THE AGES: THE INTEREST IN DETERRING POLICE MISCONDUCT VS. THE INTEREST IN PROSECUTING AND PREVENTING CRIMINAL ACTIVITY

Letting the guilty party go free? Those who are unfamiliar with the legal or criminal justice system would scoff at the idea of releasing an individual who has, for lack of a better term, been caught red-handed and dead to rights. How can a system claiming to be the epitome of all that is just and fair allow a factually guilty party to escape repercussion, and worse, escape repercussion at the hands of the system itself? The short answer would be the exclusionary rule: a prophylactic rule created by the Court with its chief focus on preventing future constitutional harms rather than repairing the immediate harm. Although the Constitution does not expressly mentioned the exclusionary rule, it is necessary to ensure that constitutional rights are protected.[130] As stated in the landmark case of *Marbury v. Madison*, "where there is a legal right, there is also a legal remedy,"[131] and

130. STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: CASES AND COMMENTARY 551 (10th ed. 2014).

131. Marbury v. Madison, 5 U.S. (1 Cranch) 137, 163 (1803).

this prophylactic rule complies with that maxim by guaranteeing that the Fourth Amendment's right to be free from unreasonable searches and seizures is not merely hollow text, but a concrete right with consequences resulting from any violation. Nevertheless, critics of the exclusionary rule can rest assured that courts are not using the rule haphazardly, but instead are performing a well thought out balancing test in deciding whether to admit or exclude evidence. Not all cases warrant the exclusion of evidence, but for the following reasons, evidence obtained from the FBI's use of the NIT should be suppressed pursuant to the exclusionary rule.

Considering the specifics and extent of the crimes at issue in the Playpen cases, at first glance it appears as if the balance between these competing interests is swayed in favor of apprehending and prosecuting the criminals, no matter the costs. However, considering the precedent a government-favorable ruling would set, it appears that the interest in deterring police conduct is at least equal to (if not greater than) the interest in prosecuting criminal behavior here, especially in light of alternative search methods the government had available.

The exclusionary rule is the scale upon which these interests are balanced. Needless to say, if the interest in deterring police misconduct outweighs the interest in prosecuting and preventing future crimes, then the balance is in favor of the exclusionary rule, and vice versa. Although the exclusionary rule would free factually-guilty individuals, there are two theories supporting its use: 1) deterrence and 2) maintaining judicial integrity.

A. *Exclusionary Rule as the Appropriate Remedy*

Under the first theory, the exclusionary rule will deter future police (or FBI) misconduct because the police will cease acting in a manner that will subsequently exclude evidence from trial and cause the case to be dismissed. While critics are correct in stating that the exclusionary rule "is not a cost-free remedy," they are incorrect in generalizing its inapplicability across the spectrum of Fourth Amendment violations.[132] Although there are other remedies that may deter police misconduct, they are not always the most applicable or appropriate for doing so. Further, even if deterrence of misconduct can be sought through other remedies, allowing illegally seized evidence to be admitted would undermine the second theory of the exclusionary rule: maintaining judicial integrity. The courts must remain insulated

132. *See* WALTER P. SIGNORELLI, THE CONSTABLE HAS BLUNDERED: THE EXCLUSIONARY RULE, CRIME, AND CORRUPTION 3-5 (2010).

from tainted evidence. If courts were to admit evidence illegally obtained, the integrity of the judiciary would be jeopardized.[133]

With the theories and competing interests of the exclusionary rule in mind, exclusion is the proper remedy here because no other remedies will redress the constitutional violation, and failure to exclude the evidence will largely expand the government's ability to anonymously hack (or search) individuals across the globe. Other possible alternatives to the exclusionary rule include civil tort claims against the officers via 42 U.S.C. § 1983, criminal prosecutions against the officers, or enactment of administrative rules allowing police departments or agencies to internally discipline officers.[134] At first glance, these alternative remedies look promising; however, their proponents appear to forget one crucial fact that pertains to the Playpen cases—the searches are performed secretly. The victims of the search had no idea that their privacy was breached until charges were brought against them, thereby removing the availability of the alternative remedies. Still, critics of the exclusionary rule would argue that the alternative remedies only become available after the government's alleged constitutional violation and when the suspect is apprehended; and that these remedies are sufficient enough to deter police misconduct without allowing the guilty party to be released. However, in their haste to argue for the elimination of the exclusionary rule, critics either forget or are unwilling to see that the exclusionary rule can operate either directly, by excluding evidence produced from a constitutional violation, or indirectly, by preventing the government from operating in a manner contrary to the Constitution out of fear that any evidence obtained would result in suppression at a subsequent trial.

Additionally, the exclusionary rule operates to benefit not only those who are factually guilty, but innocent parties as well. When the government is operating covertly and searching individuals without their knowledge, the risk of factually-innocent parties being searched increases. The FBI infected (or searched) over 8,000 computers with malware and "870 arrests were made in connection with the case."[135] Assuming these numbers are correct, it appears that at least 7,130 individuals were unaware that their computers were hacked by the FBI. Here, where other remedies fail, the exclusionary rule would prevent surreptitious, international hacking by the FBI.

---

133. SALTZBURG, *supra* note 130, at 553.

134. *Alternatives to the Exclusionary Rule*, JUSTIA, https://law.justia.com/constitution/us/amendment-04/32-alternatives-to-the-exclusionary-rule.html [https://perma.cc/S9QE-2FDX].

135. *900 Suspected Pedophiles Arrested as 'Darknet' Child Porn Kingpin Jailed for 30yrs*, RT (May 6, 2017, 3:28 PM), https://www.rt.com/news/387317-pedophile-ring-arrested-playpen/ [https://perma.cc/32QX-ZHCG].

B. *The Government's Incompatible Interests: A Tradeoff of Public Safety for Continued Hacking Ability*

In an effort to limit the breadth of governmental searches, Judge Richard Posner once stated in *United States v. Evans*, "[i]f they are looking for a canary's corpse, they can search a cupboard, but not a locket."[136] However, in the event that any Playpen case results in the Supreme Court finding that suppression is not warranted, that quote will become meaningless. "[W]hile some courts have at times allowed 'roving wiretaps' (which name specific persons but not places) and 'all persons' warrants (which name specific places but not specific persons), *no* court has previously upheld the issuance of a warrant to search unknown persons in unknown places."[137] If the Supreme Court or any circuit court passes on the opportunity to admonish the government's unfettered use of the NIT, the government will not limit remote accessing of computers to cases containing sympathetic facts, but instead utilize the NIT for the most menial crimes simply because they can. If past behavior is the best indicator of future behavior, look no further than to the government's use of a Stingray device to locate and apprehend a suspect who stole less than $57 worth of fast food.[138] The use of a Stingray device to track suspects was first thought of as a practical method for maintaining national security and eliminating terrorist threats; however, there is little evidence to suggest that the government is using the Stingray for national security. Instead, it is mostly used for low-level crimes, with the word "terrorism" appearing only on applications for funding grants.[139] Similarly, what now appears as the only method for locating anonymous distributers of child pornography can later be used to identify those engaging in low-level crimes, such as online gambling in any state that prohibits it.

In some of the Playpen prosecutions, the government appeared to have incompatible interests. On one hand, they claimed that the FBI's use of the NIT was necessary for public safety because without it they could not identify, locate, and apprehend individual Playpen members. On the other hand, the FBI's interest in public safety was outweighed by their interest in keeping the NIT's source code secret. Instead of complying with Judge Robert Bryan's order in *United*

136. SALTZBURG, *supra* note 130, at 160 (quoting United States v. Evans, 92 F.3d 540 (7th Cir. 1996)).

137. Crocker, *supra* note 3.

138. Tim Cushing, *Your Tax Dollars at Work: Cops Use Stingray to ALMOST Track Down Suspected Fast Food Thief*, TECHDIRT (May 11, 2016, 12:42 PM), https://www.techdirt.com/articles/20160507/11342334371/your-tax-dollars-work-cops-use-stingray-to-almost-track-down-suspected-fast-food-thief.shtml [https://perma.cc/6DNX-57VF].

139. *Id.*

States v. Michaud[140] to disclose the NIT source code to the defense, the prosecutors in Washington dropped all charges against Jay Michaud.[141] If the government's goal is to actually enforce the law and maintain public safety, they clearly failed by not disclosing to the defendant a portion of the source code or even how the NIT operates.[142] Ultimately, the government is asking that courts take their word as true that the NIT operates safely and causes minimal intrusion to computers. However, without the code, only assumptions can be made.

VI. RESTORING JUSTICE AND INTEGRITY TO THE CRIMINAL JUSTICE SYSTEM IN AN AGE OF DIGITAL COMMUNICATION: REMEDYING THE GOVERNMENT'S LIMITLESS SEARCH OF UNKNOWN INDIVIDUALS

Contrary to the viewpoints expressed by the government and the "Affidavit In Support Of Application For Search Warrant," there are alternative methods to locate individuals using anonymity software (like using Tor) that are not as intrusive or harmful. Remote accessing software that inflicts malware, such as the NIT, carries potential consequences that do not necessarily exist in the physical world. A house will not crash from being broken into, whereas a computer might.[143] The NIT gave the FBI complete control over the computer, which could have corrupted the operating system (causing all files to be destroyed) or caused other unanticipated problems.[144] Instead of permitting future dragnet searches, such as the one employed by the FBI during the Playpen investigations, there are at least four potential options available which would allow technological searches to comport with the Fourth Amendment and jurisdictional requirements: 1) the FBI could conduct their investigation and locate anonymous individuals in a way that would not be considered a search, thereby eliminating any constitutional concerns;[145] 2) Congress could enact a specific statute that would address exactly where, when, and how the government could remotely access computers;[146] 3) the gov-

140. United States v. Michaud, Case No. 3:15-cr-05351-RJB, 2016 WL337263 (W.D. Wa. Jan. 28, 2016).

141. Cyrus Farivar, *To Keep Tor Hack Source Code Secret, DOJ Dismisses Child Porn Case*, ARSTECHNICA (Mar. 5, 2017, 2:30 PM), https://arstechnica.com/tech-policy/2017/03/doj-drops-case-against-child-porn-suspect-rather-than-disclose-fbi-hack/ [https://perma.cc/JHX8-P8Q5].

142. *See* Jenna McLaughlin, *FBI Chooses Secrecy over Locking up Criminals*, THE INTERCEPT (May, 2, 2016, 8:14 AM), https://theintercept.com/2016/05/02/fbi-chooses-secrecy-over-locking-up-criminals/ [https://perma.cc/G4G5-ZYH9].

143. Zetter, *supra* note 8.

144. Interview with Angel A. Daruna, *supra* note 6; Zetter, *supra* note 8.

145. Robert Graham, *Orin's Flawed Argument on IP Address Privacy*, ERRATA SECURITY (Dec. 7, 2016), http://blog.erratasec.com/2016/12/orins-flawed-argument-on-ipaddress.html#.WRv5NIWcGUk [https://perma.cc/W3V3-GD7A].

146. Zetter, *supra* note 8.

ernment can offer specific details about what they know at the time they seek a warrant; and 4) Congress can appoint specialized courts to determine probable cause and issue warrants relating to technological searches. All of these options provide the criminal justice system with an avenue for courts to keep up with the advancement in technology without having to dismiss cases due to government investigations running afoul of the Constitution. As Andrew Crocker, a staff attorney for the Electronic Frontier Foundation, stated: "This is more than just requiring the government to jump through hoops—[it is] what stands between a constitutional, particularized search and precisely the type of generalized warrant the Fourth Amendment was designed to prevent."[147]

First, the easiest way to avoid a constitutional violation would be to operate in a manner that does not classify as a search under the Fourth Amendment. If the FBI does not intrude into an area upon which an individual has a reasonable expectation of privacy, the costlier alternatives to the NIT are not necessary. In fact, the NIT itself would not be necessary. Agent Macfarlane confused *necessary* with *convenient* when he informed Judge Buchanan, via the affidavit, that the NIT was the only method that would reveal the identities of the Playpen members. Instead of using malware to infect a member's computer, the FBI could have posted a Word or PDF document on Playpen with an image tag that, once clicked, would direct the member's computer to the FBI's server.[148] According to Robert Graham, a frequent blogger on Errata Security, an Adobe "Acrobat [or] Word program [is not] protected by Tor. [A member's] computer will then contact the FBI's server looking for the image, revealing their public IP address."[149] Under Graham's scenario, the government would not be hacking Playpen members' computers but instead allowing them to contact the FBI. Therefore, such voluntary contact would not amount to governmental compulsion, and thus, there would be no intrusion upon a reasonable expectation of privacy.

Second, just as Congress did with wiretapping, it could enact a specific statute that would govern how the government could remotely access suspects' computers. The "procedural" amendment to Rule 41 is too short to govern something as expansive as global hacking. Remote accessibility of thousands of computers is something that Congress should address. In fact, some members of Congress have introduced legislation that would repeal the new amendments to Rule 41 (such as the "Stopping Mass Hacking Act").[150]

147. Crocker, *supra* note 25.

148. Graham, *supra* note 145.

149. *Id.*

150. Stopping Mass Hacking Act, H.R. 1110, 115th Cong. § 2 (2017).

Third, the government could be—and should have been—more specific with the information relating to the target of the search, especially when the target conceals its identity. Because the FBI was running Playpen for two weeks, agents could have obtained detailed information regarding specific members and their usage patterns.[151] If the FBI had provided specific information and sought a warrant to search each member, the FBI would have most likely met the particularity requirement by providing the magistrate with as much information as possible for each individualized search warrant. Instead, the FBI mislead Judge Buchanan into believing that there were no means of obtaining individualized identification in an attempt to receive a general warrant so that they would have as much freedom to operate as possible.

Lastly, under Article III, Congress can "ordain and establish"[152] specialized courts that can focus solely on technology-based searches, whether it be wiretapping, tracking, or hacking, just to name a few. Although Congress is most likely unwilling to appropriate funds to establish such a specialized court, it would greatly reduce the risk of unconstitutional invasions of privacy. The magistrates that are currently issuing warrants are out of touch and unfamiliar with how modern technology operates. Just as Judge Buchanan may have been misled, other magistrate judges will continue to be as well.

VII. CONCLUSION

Some of the Playpen courts' ends-justify-the-means mentality compromises the integrity of the balance between the two models of criminal justice jurisprudence (crime control and due process). Holdings such as these turn back the clock and risk sending the United States into the pre-revolutionary era. History tends to repeat itself, and it appears that warrants resembling the NIT are nothing more than general warrants concealed in cyberspace.

There is no mistaking that the advancement of technology incites the advancement of crime. Although, on the surface, it appears that courts denying suppression are keeping up with and combating new criminal operations, in effect they are achieving the opposite. These holdings blur the line between criminal behavior and proper police conduct. It would be hypocritical to expect U.S. citizens to comply with the law when the judiciary is giving the government a pass whenever it deems that the facts warrant the constitutional deviation.

---

151. Crocker, *supra* note 3.

152. U.S. CONST. art. III, § 1.