The Fourth Amendment and the Dark Web: How to Embrace a Digital Jurisprudence that Protects Individual Liberties

McKENZIE HIGHTOWER*

INTRODUCTION

> The dark net is a world of power and freedom: of expression, of creativity, of information, of ideas. Power and freedom endow our creative and our destructive faculties. The dark net magnifies both, making it easier to explore every desire, to act on every dark impulse, to indulge every neurosis.
> –Jamie Bartlett[1]

A tip in February 2015 set off a chain of remarkable events that eventually led the Federal Bureau of Investigation (FBI) to a child pornography website on the dark web named "Playpen."[2] However, the FBI did not shut down the website right away.[3] Instead, the FBI operated the website for two weeks to identify website users.[4] Law enforcement eventually applied for a warrant in the Eastern District of Virginia to use the Network Investigative Technique (NIT) to identify Playpen's users and administrators.[5] The NIT can be thought of as a form of malware because it gains access to a suspect's computer without his or her consent. Specifically, the NIT collects the target computer's "Host Name," operating system, IP address, and "Media Access Control" address as well as other information.[6] This was a risky and controversial plan because it required the government to operate a child pornography website. To obtain a warrant, law enforcement prepared an affidavit documenting its basis for probable cause and the urgent need to identify some of the 150,000 users exploiting children on the website.[7] However, the application did not—and could not—state with particularity

---

* Georgetown University Law Center, J.D. 2021. © 2021, McKenzie Hightower. I would like to thank the editors of *The Georgetown Law Journal Online* for volunteering their time and reading this piece with such close attention. It is such an honor to publish with the *Journal*.

[1] JAMIE BARTLETT, THE DARK NET: INSIDE THE DIGITAL UNDERWORLD 237 (2015).

[2] Kurt C. Widenhouse, *Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to Be Found*, 13 J. BUS. & TECH. L. 143, 143 (2017).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.* at 144.

[7] *See id.* at 143; *see also 'Playpen' Creator Sentenced to 30 Years*, FED. BUREAU OF INVESTIGATION (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years [https://perma.cc/C8DQ-9Q9W] (explaining that the website had over 150,000 users).

the places to be searched because it was unknown where the users of Playpen were located due to their use of Tor, an anonymizing software.[8]

The court issued a search warrant, and law enforcement sent malware using the NIT to a user's computer when the user accessed the Playpen website.[9] The malware caused the user's computer to send identifying information to federal agents in the Eastern District of Virginia.[10] After the NIT warrant was issued, the FBI obtained over 9,000 IP addresses across 120 countries from users logging in to Playpen.[11] As a result of this sting, over 200 users were criminally charged, and forty-nine American children were rescued from exploitation.[12] Because suspects were discovered outside the Eastern District of Virginia, however, courts have debated whether the magistrate judge exceeded his authority by issuing a warrant outside his jurisdiction.[13]

---

[8] *See* Widenhouse, *supra* note 2, at 154 (discussing the issue of jurisdictional legality of the Virginia warrant when a defendant in Pennsylvania used Tor to mask his location). To read more about Tor, see *infra* Part I. To read more about the problems that a lack of a specific location on the dark web poses for law enforcement, see *infra* Part I.B.

[9] *See* Widenhouse, *supra* note 2, at 144.

[10] *See id.*

[11] *See* Cara Tabachnick, *The Pitfalls of Policing the Dark Web*, WORLD POL. REV. (Jan. 9, 2019), https://www.worldpoliticsreview.com/articles/27136/the-pitfalls-of-policing-the-dark-web [https://perma.cc/73PW-PG3A].

[12] *See* Thomas Brewster, *Exclusive: What Happened When the FBI Took Over the Instagram and Kik of a Child Porn Dealer*, FORBES (Mar. 6, 2019, 10:31 AM), https://www.forbes.com/sites/thomasbrewster/2019/03/06/exclusive-the-fbi-took-over-the-online-identity-of-a-pedophile-letting-child-porn-spread-for-18-months/.

[13] *Compare* United States v. McLamb, 880 F.3d 685, 690–91 (4th Cir. 2018) (holding the Eastern District of Virginia was "the most sensible single district" for the Playpen warrant location), United States v. Duncan, No. 3:15-CR-00414-JO, 2016 WL 7131475, at *4 (D. Or. Dec. 6, 2016) (denying suppression because agents acted in good faith), United States v. Lough, 221 F. Supp. 3d 770, 783 (N.D.W. Va. 2016) (denying suppression because defendant had no expectation of privacy, technology was like a tracking device, and good faith exception applied), *aff'd*, 721 F. App'x 291 (4th Cir. 2018), United States v. Kienast, No. 16-CR-103, 2016 WL 6683481, at *4 (E.D. Wis. Nov. 14, 2016) (denying suppression because malware was like a tracking device), *aff'd*, 907 F.3d 522 (7th Cir. 2018), United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *11 (W.D. Mo. Oct. 20, 2016) (denying suppression because no expectation of privacy in an IP address), *aff'd*, 770 F. App'x 324 (8th Cir. 2019), *and* United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016) (denying suppression because malware was like a tracking device), *aff'd*, 721 F. App'x 304 (4th Cir. 2018), *with* United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, at *5, *20 (D. Minn. Mar. 23, 2017) (finding the good faith exception does not apply to the Playpen warrant), *aff'd*, 769 F. App'x 400 (8th Cir. 2019), United States v. Croghan, 209 F. Supp. 3d 1080, 1090 (S.D. Iowa 2016) (granting suppression because warrant exceeded judge's authority), *rev'd sub nom.* United States v. Horton, 863 F.3d 1041 (8th Cir. 2017), United States v. Workman, 205 F. Supp. 3d 1256, 1263 (D. Colo. 2016) (same), *rev'd*, 863 F.3d 1313 (10th Cir. 2017), United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *35–36 (N.D. Okla. Apr. 25, 2016) (granting suppression because warrant exceeded judge's authority), *and* United States v. Levin, 186 F. Supp. 3d 26, 44 (D. Mass. 2016) (same), *vacated*, 874 F.3d 316 (1st Cir. 2017).

To remedy this debate, the drafters of the Federal Rules of Criminal Procedure (FRCP) modified Rule 41 to explicitly allow future digital out-of-district searches under certain circumstances.[14] Before its modification in 2016, FRCP 41(b) designated five scenarios in which a federal magistrate judge may issue a warrant.[15] "Subsection (b)(1) states the general rule that, 'a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located in the district.'"[16] The subsequent four subsections provide that a judge has authority to issue a warrant *outside* his or her district

> (2) if the person or property is located within the district but might move or be moved outside the district before the warrant is executed; (3) if the magistrate judge sits in a district in which activities related to terrorism have occurred; (4) to install a tracking device within the district, though the magistrate judge may authorize the continued use of the device if the person or object subsequently moves outside of the district; and (5) where the criminal activities occur in the District of Columbia, any United States territory, or on any land or within any building outside of the country owned by the United States or used by a United States diplomat.[17]

After the Playpen cases, the drafters of the FRCP voted to add a new provision to Rule 41.[18] This amendment allows magistrate judges to issue search warrants *outside* their jurisdictions, in limited circumstances, even when the activities do not originate in their jurisdictions as required under Rule 41(b)(1)–(5).[19] The amendment, now Rule 41(b)(6), reads,

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located *has been concealed through technological means* . . . .[20]

---

[14] *See* Widenhouse, *supra* note 2, at 148.
[15] *Id.* at 146–47.
[16] *Id.* (quoting FED. R. CRIM. P. 41(b)(l)).
[17] *Id.* at 146–47 (quoting FED. R. CRIM. P. 41(b)(2)–(5)).
[18] *See* COMM. ON RULES OF PRACTICE AND PROC. OF THE JUD. CONFERENCE OF THE U.S., REPORT OF THE ADVISORY COMMITTEE ON CRIMINAL RULES 47, 54 (2015) [hereinafter COMM. REPORT].
[19] *See* Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches,* U.S. DEP'T OF JUST. (June 20, 2016), https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches [https://perma.cc/C8ZP-UM73].
[20] FED. R. CRIM. P. 41(b)(6) (emphasis added).

The drafters gave one overriding reason for this modification: they worried about a "situation [where] the warrant sufficiently describes the computer to be searched, but the district within which the computer is located is unknown."[21] Of importance for this Note, the drafters explicitly stated that "[t]he proposed amendment *does not address constitutional questions* that may be raised by warrants for remote electronic searches, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information."[22] This Note will specifically address the constitutional question the drafters declined to answer and endeavor to ensure that individual liberty is balanced with the need to seek justice for those who use the dark web maliciously.

This Note will proceed in three Parts. Part I will lay out how the dark web and surface web interact with the Fourth Amendment. Part II will then show how a traditional conception of the Fourth Amendment, specifically the particularity requirement, is incompatible with the new digital age. Part III will specifically focus on the dark web, building on past process-based approaches to the Fourth Amendment and applying them to the dark web in a way that allows law enforcement to conduct its duties while also ensuring individual liberties. This Part will use the implications of the modified Rule 41 to show how courts are already using this approach—what I call the "liminal approach"—to redefine the Fourth Amendment in the digital age.

I. THE DARK WEB AND THE SURFACE WEB

The Internet we all know—the one with Yelp, Facebook, and Amazon—is only the surface web.[23] It is indexed and searchable through resources like Google.[24] This surface web "is just the tip of the proverbial iceberg because most of the Internet 'is submerged below.'"[25] "This un-indexable part of the Internet is known as the 'deep web' which refers to everything [that] *cannot* be found via search engines."[26] The dark web is part of the deep web.[27]

---

[21] *See* COMM. REPORT, *supra* note 18, at 54. The committee goes on to specifically identify "persons sending fraudulent communications to victims and child abusers sharing child pornography may use proxy services designed to hide their true IP addresses" as its primary concern under this first rationale. *Id.*

[22] *Id.* at 55–56 (emphasis added).

[23] *See Clearing Up Confusion— Deep Web vs. Dark Web*, BRIGHTPLANET (Mar. 27, 2014) [hereinafter *Clearing Up*], https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/ [https://perma.cc/QGD3-B87Y].

[24] *Id.*

[25] Kaleigh E. Aucoin, *The Spider's Parlor: Government Malware on the Dark Web*, 69 HASTINGS L.J. 1433, 1440 (2018).

[26] *Id.*

[27] *Id.*; *Clearing Up*, *supra* note 23.

Projected to be around 1,000 times bigger than the indexed web,[28] the dark web can only be visited with special encryption software like Tor's.[29] Tor, also known as "The Onion Router," allows users to anonymize their Internet Protocol (IP) addresses, so no one can trace their locations.[30] As illustrated in Figure 1 below, Tor does this by routing a user's IP address through a network of different nodes, thus obscuring the user's original location.[31]

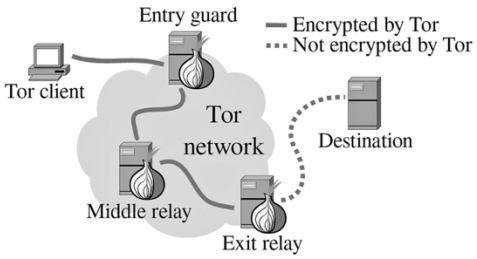

Figure 1

Tor was originally developed by the United States Naval Research Laboratory in the 1990s to shield government communications.[32] Now, Tor is funded by the United States Department of State, and it is maintained by a nonprofit organization called the Tor Project.[33]

---

[28] Ben Rossi, *Why It's Not Impossible to Police the Dark Web*, INFORMATION AGE (Nov. 17, 2015), https://www.information-age.com/why-its-not-impossible-police-dark-web-123460505/ [https://perma.cc/2NM9-28UD].

[29] THOMAS OLOFSSON, INTELLIAGG, DEEP LIGHT—SHINING A LIGHT ON THE DARK WEB 5 (2016), https://onyxcomms.com/wp-content/uploads/2017/01/intelliagg-deeplight-report.pdf [https://perma.cc/3PNM-UCLC].

[30] *Id.*; *see What Is Tor?*, ELEC. FRONTIER FOUND., https://www.eff.org/torchallenge/what-is-tor.html [https://perma.cc/5BDE-XA5K] (last visited April 12, 2021) (explaining Tor through an illustration titled "Octopus Not So Great!" by Molly Crabapple and John Leavitt).

[31] *What is a Tor Relay?*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/what-tor-relay#:~:text=Tor%20relays%20are%20also%20referred,%2C%20exit%20relays%2C%20and%20bridges [https://perma.cc/U4JY-6UE9]. Figure 1 originates from Aditya Tiwari, *Everything About Tor: What Is Tor? How Tor Works?*, FOSSBYTES (Aug. 17, 2020), https://fossbytes.com/everything-tor-tor-tor-works/ [https://perma.cc/RHW4-9YS4].

[32] Widenhouse, *supra* note 2, at 145.

[33] *See Tor: Myths and Facts*, ELEC. FRONTIER FOUND., https://www.eff.org/document/tor-myths-and-facts [https://perma.cc/W5ZW-2QDL] (last visited Mar. 20, 2020); *see also* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), https://www.wired.com/2014/08/operation_torpedo/ [https://perma.cc/7DSH-DJZL].

On the dark web, websites end in ".onion"[34] and have "theoretically untraceable" physical locations.[35] These physical locations are "nearly impossible to trace" because the websites are masked behind layers of interlinked computers like layers of an onion.[36] There are both legitimate and illicit uses for the dark web. Legitimate uses include protection from different types of surveillance,[37] the power to circumvent government censorship and surveillance,[38] and the ability to communicate with journalists about highly sensitive information on secret government operations.[39] On the other hand, illicit uses for the dark web include, *inter alia*, child pornography,[40] money laundering,[41] and drug[42] and human trafficking.[43]

---

[34] *See* Tom Simonite, *"Dark Web" Version of Facebook Shows a New Way to Secure the Web*, M.I.T. TECH. REV. (Nov. 3, 2014), https://www.technologyreview.com/s/532256/dark-web-version-of-facebook-shows-a-new-way-to-secure-the-web/ [https://perma.cc/9QZL-EDJL].

[35] Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY (Sept. 16, 2014), https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/ [https://perma.cc/F4XU-X2P7]; *see also* Jesse Atlas, Opinion, *Insider Trading on the Dark Web*, FORBES (Mar. 25, 2014, 8:00 AM), https://www.forbes.com/sites/realspin/2014/03/25/insider-trading-on-the-dark-web/#1e3674d46a61 ("Without an IP address, it is nearly impossible to trace users back to their computers. Thousands of people evaded the FBI by using the Tor browser to do illicit deals on sites like The Silk Road—the [eBay] for drugs, guns, and hit men.").

[36] *See* Atlas, *supra* note 35.

[37] *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1087 (2017) (discussing how Tor provides protection from two different types of surveillance: traffic analysis and acquisition of metadata); *see also* Mike Tigas, *A More Secure and Anonymous ProPublica Using Tor Hidden Services*, PROPUBLICA (Jan. 13, 2016, 10:45 AM), https://www.propublica.org/nerds/a-more-secure-and-anonymous-propublica-using-tor-hidden-services [https://perma.cc/MN3D-Q4NB] (providing that a hidden service version of ProPublica was launched to protect readers from surveillance because "readers should never need to worry that somebody else is watching what they're doing on [the website]").

[38] *See* David Talbot, *Dissent Made Safer*, M.I.T. TECH. REV. (Apr. 21, 2009), https://www.technologyreview.com/s/413091/dissent-made-safer/ [https://perma.cc/D4E4-85M8] (discussing how Tor has enabled users to circumvent government censorship and surveillance).

[39] *See* Sarah Volpenhein, *Dark Web Poses Challenges for Law Enforcement*, GOV'T TECH. (Aug. 10, 2015), https://www.govtech.com/gov-experience/Dark-Web-Poses-Challenges-for-Law-Enforcement.html [https://perma.cc/MGW2-MJ69] (explaining that, according to a congressional report, "[f]ormer CIA contractor Edward Snowden reportedly used an operating system that automatically [ran] Tor to communicate with journalists and leak classified information on the United States' mass surveillance programs").

[40] *See, e.g.*, Amanda Haasz, *Underneath It All: Policing International Child Pornography on the Dark Web*, 43 SYRACUSE J. INT'L L. & COM. 353, 354 (2016).

[41] *See, e.g.*, Fiammetta Piazza, *Bitcoin in the Dark Web: A Shadow over Banking Secrecy and a Call for Global Response*, 26 S. CAL. INTERDISC. L.J. 521, 522 (2017).

[42] *See, e.g.*, Thomas J. Nugent, *Prosecuting Dark Net Drug Marketplace Operators Under the Federal Crack House Statute*, 88 FORDHAM L. REV. 345, 346–47 (2019).

[43] *See, e.g.*, Charles Graeber, *The Man Who Lit the Dark Web*, POPULAR SCI. (Aug. 30, 2016), http://www.popsci.com/man-who-lit-dark-web [https://perma.cc/K2WR-2A2H].

Recently, the government launched an effort to de-anonymize the dark web in a variety of ways. The most traditional technique the government uses is infiltrating criminal rings on the dark web through undercover online operations.[44] However, law enforcement also uses Memex, a program created by the U.S. Defense Advanced Research Projects Agency, to scrape and index millions of pages on the dark web.[45] Finally, another technique is "Sweetie." "Sweetie is an Internet avatar—a computer-animated, photorealistic image of a ten-year-old Filipina girl"—that is used to lure individuals out onto the surface web for identification.[46] Of primary importance for this Note, the government has also begun to use NITs.[47]

With the rise of these new investigative tools, existing law has struggled to keep up. Fourth Amendment analyses have been difficult to translate to digital evidence—especially with respect to activity on the dark web. According to prominent scholar Orin S. Kerr, traditional analyses often make little sense and can lead to absurd results:

> Digital evidence exposes the contingency of the existing rules. It reveals how the rules generated to implement constitutional limits on evidence collection are premised on the dynamics of physical crimes and traditional forms of physical evidence and eyewitness testimony. When those implementing rules are applied to the facts of digital evidence collection, they no longer remain true to the purpose they were crafted to fulfill. Digital evidence changes the basic assumptions of the physical world that led to the prior rules, pointing to results that no longer reflect the basic goals and purposes of the Fourth Amendment.[48]

This disconnect is not surprising—the law has often trailed technological advancement. Nonetheless, as articulated below, the digital age is a watershed moment for the Fourth Amendment and for the particularity requirement specifically. The Fourth Amendment needs to be "translated"[49] with a foundation in the digital world—not the physical world—for digitally-based evidence. This would require altering key doctrines like the particularity requirement and the jurisdictional requirement.[50] Below, Sections

---

[44] *See* Sophia Dastagir Vogt, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 SANTA CLARA J. INT'L L. 104, 117 (2017).
[45] *See* Anthony Cuthbertson, *Death of the Dark Web? DARPA's Memex Search Engine Allows Tor Tracking*, INT'L BUS. TIMES (Feb. 16, 2015, 1:38 PM GMT), http://www.ibtimes.co.uk/death-darkwebdarpas-memex-search-engine-allows-tor-tracking-1488124 [https://perma.cc/H9M3-L6Z6].
[46] Whitney J. Gregory, *Honeypots: Not for Winnie the Pooh but for Winnie the Pedo: Law Enforcement's Lawful Use of Technology to Catch Perpetrators and Help Victims of Child Exploitation on the Dark Web*, 26 GEO. MASON L. REV. 259, 279–80 (2018).
[47] *See* Vogt, *supra* note 44, at 115–16.
[48] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 306 (2005).
[49] For more on the concept of translation, see *infra* Part II.
[50] For more on this concept, see *infra* Part III.

A and B discuss how the Internet has been perceived from multiple perspectives and document how the surface web and the dark web complicate traditional Fourth Amendment analysis.

A. THE CHALLENGES OF THE SURFACE WEB

As an initial matter, Orin Kerr and this author agree that there are two views of the surface web, the internal perspective and the external perspective.[51] The "internal perspective" accepts the virtual world of cyberspace as akin to reality.[52] More specifically, "[t]he internal perspective adopts the point of view of a user who is logged on to the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct."[53] This perception is best thought of as a first-person perspective. For instance, one might imagine shopping on the Internet as comparable to walking into a physical store, or one might imagine writing a private document and storing it on a computer as akin to handwriting the same letter and tucking it into a drawer.[54] The second perspective, called the "external perspective," views the digital world from a functionality-based vantage point. [55] "The external perspective adopts the viewpoint of an outsider concerned with the functioning of the network in the physical world rather than the perceptions of a user."[56] Unlike the physical world, where a house is always a house, no matter what perspective one employs, the result of a digital search changes based on which of these two perspectives of the surface web one employs.[57] Kerr believes these perspectives are dichotomies, and he conceptualized them in reference to search and seizure law.[58] In this Part, this Note discusses how the internal/external perspectives inform the dark web and the surface web in the context of search and seizures, but in Part II, the Note brings the internal/external perspectives to bear on the particularity requirement.

There are several obvious yet notable challenges in receiving a search warrant for the surface web. Most evidently, there are no geographical borders on the Internet, so the "crime scene" occurs in multiple places at once.[59]

---

[51] Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 359–60 (2003).
[52] *Id.* at 359.
[53] *Id*.
[54] *See id.* at 359–360.
[55] *Id.* at 360.
[56] *Id.*
[57] *See id*. at 360–61 ("[T]echnology in a sense leaves us with two Internets, rather than one.").
[58] *Id*. at 364–68.
[59] *See* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 98 (2001) (noting that for investigators of Internet crimes, there are no geographical borders and thus no "traditional crime scene"). Such a view depends on which perspective of the Internet one takes, internal or external. The choice forces the judge to choose between important competing interests. For more on how this

This makes it more difficult to approve a warrant for one specific location, but it also complicates traditional notions upon which the Fourth Amendment was built. For example, if a bank was robbed by a hacker, and the perpetrator redirected his IP address through dozens of computers to hide himself, is each computer a crime scene? Is this crime a conspiracy because he employed the help of multiple persons' computers? Has he crossed interstate lines?[60] If one's use of the Internet always crosses state lines, then is the external perspective of the Internet—viewing it as just wires and cords—the correct perspective?

In addition, identifying a particular account or IP address almost never identifies the perpetrator because it is unknown who used the address.[61] There is always the inferential step of assuming the owner of the email account was the one that committed the crime, not her daughter or father, or anyone else who might also have had access to the account. While other physical crimes could pose similar problems (such as inferring the individual who bought all the materials for a bomb intended to make a bomb), such crimes do not *always* rely on circumstantial evidence in the same way that Internet crimes tend to.[62]

There is also a loss of "the distinction between [impermissible] inside surveillance and [permissible] outside surveillance."[63] The Fourth Amendment jurisprudence often bases its protections on whether the disputed space is a low-privacy, public (outside) space or a high-privacy, private (inside) space.[64] Under this physical conception of Fourth Amendment protection, "the inside/outside distinction creates the basic balance of Fourth Amendment law," allowing police to investigate low-privacy, public areas and allowing individuals to retain individual liberties in high-privacy places.[65] However, this distinction does not apply well to the surface web. For example, even though one could intuitively think there is an

---

choice effects individual liberties and how the liminal approach forces judges to name the choices they make, see *infra* Part III.

[60] Under current law, the use of a computer for certain activities constitutes interstate commerce. *See, e.g.*, 18 U.S.C. §§ 2252, 2252A (2018) (stating that interstate commerce includes the exploitation of minors or distribution of child pornography through the use of computers).

[61] According to the 2002 version of the Justice Department's digital investigative manual, "generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it." ORIN S. KERR & COMPUT. CRIME AND INTELL. PROP. SECTION CRIM. DIV., U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 90–91 (2002).

[62] *See* MICHELLE KANE, U.S. DEP'T OF JUST., PUTTING THE SUSPECT AT THE COMPUTER 4, http://www.oas.org/juridico/english/cyb_pan_user_en.pdf [https://perma.cc/ED74-GSBL] (last visited Jan. 16, 2021).

[63] Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1009 (2010).

[64] *See id.* at 1017–18.

[65] *Id.*

internal/external distinction between one's public-facing Facebook page and one's private browsing history, in cases relevant to national security, the law considers them both available to government perusal without a warrant.[66] Additionally, even when courts do find some semblance of privacy in the digital world, other exceptions to Fourth Amendment protection usually protect the government's ability to prosecute accused criminals.[67] Thus, the Fourth Amendment's protections break down in the digital world.

Moreover, because there are no geographical limits to the Internet, everything is now in "plain view" for law enforcement to inspect or search as long as the data was placed on the computer "in a publicly-accessible manner."[68] There is virtually no limit on the amount of data law enforcement may sift through,[69] which, while not a new problem, makes "[c]omputer search warrants [] the closest things to general warrants we have confronted in the history of the Republic."[70] Because the Fourth Amendment was designed to safeguard against such general warrants,[71] computer warrants are yet another instance where the digital world breaks down key underpinnings of the Fourth Amendment and its focus on what exists physically.

---

[66] David Ingram, *Can the Government Look at Your Web Habits Without a Warrant? Senators Hope to Clarify That*, ABC NEWS (May 15, 2020, 2:30 PM), https://www.nbcnews.com/tech/security/can-government-look-your-web-habits-without-warrant-senators-hope-n1207936 [https://perma.cc/M6ZN-J7KL]. Law enforcement can still obtain Facebook data without a warrant in cases that do not involve national security when law enforcement says a case involves death or "potential bodily harm." However, Facebook grants "emergency requests" that are outside of the normal legal process for warrants when there is a claim that "potential bodily harm" or death is involved. Ella Fassler, *Here's How Easy It Is for Cops to Get Your Facebook Data*, ONE ZERO (June 17, 2020), https://onezero.medium.com/cops-are-increasingly-requesting-data-from-facebook-and-you-probably-wont-get-notified-if-they-5b7a2297df17 [https://perma.cc/UC7Z-ACPQ]. The rates of such requests have skyrocketed; "[i]n 2019, the government made 6,447 such 'emergency requests,' compared to 6,000 in 2018 and 3,672 in 2017." *Id*.

[67] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 284, 292 (6th Cir. 2010) (holding that the good faith exception to the Fourth Amendment protected the government from suppression even though the court found that the defendant had a reasonable expectation of privacy in his emails).

[68] *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 84 (1994).

[69] Kerr, *supra* note 63, at 1013 ("Traditional Fourth Amendment rules have been crafted in light of those assumptions; the rules generally are scale- and location-specific. Those assumptions do not hold in the Internet environment. In a world of data, third-party services can always provide more data, and the data can be anywhere. No limit exists on the number, size, or location of accounts, services, or data one person can control that might contain the evidence that the government seeks."). Even when courts have attempted to place restrictions on cyber search warrants, scholars have still called the restrictions unlawful. *See* Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. BRIEF 1, 1–2 (2011).

[70] Ohm, *supra* note 69, at 11.

[71] *See infra* Part II.

And because the Fourth Amendment is rooted in the injustice of depriving an individual of property without judicial process, the government could—and does—circumvent this prohibition by creating an exact digital copy of a computer and leaving the original computer with the suspect.[72] Thus, no "meaningful interference with an individual's possessory interests in that property" occurs.[73] However, legal intuition tells us that if the police took a person's diary, transcribed every word magically within milliseconds before returning the diary back to that person, and then the police took months—if not years—to comb through the transcription for clues to a crime, individual Fourth Amendment rights have been violated.[74] Possessory interests might not have been violated, but deeper, ethical and judicial conceptions underlying the privacy protections of the Fourth Amendment have been violated. By basing most, if not all, conceptions of the Fourth Amendment in the physical realm, such truths or analyses are often overlooked. Thus, although the existing scholarship mines the depths of the problems that the surface web poses for a traditional notion of the Fourth Amendment, this Note offers a novel analysis of the ways that the dark web is incompatible with existing Fourth Amendment conceptions.

B. THE CHALLENGES OF THE DARK WEB

For years, scholars have debated whether judges should apply the traditional approach to the Fourth Amendment or develop a novel approach for the surface web.[75] But few scholars have explored the even more drastic differences between physical evidence gathering and dark web investigations. Unlike on the surface web, on the dark web, no information transmitted to third parties is accessible, so digital footprints are not only obscured but also functionally nonexistent without complex government malware.[76] This is akin to a physical theft occurring without a single trace of evidence left behind. As of the time of this writing, no other paper explores the dark

---

[72] Kerr, *supra* note 48, at 301.
[73] *Id.* (quoting United States. v. Jacobsen, 466 U.S. 109, 113 (1984)).
[74] *See* Stanford v. Texas, 379 U.S. 476, 485 (1965) (emphasizing that a warrant must specify the ideas contained in the book to be seized).
[75] *Compare* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 766 (2005) (rejecting Professor Kerr's belief that legislatures provide more comprehensive privacy protections in response to technological innovation), *and* David J. S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 842 (2005) ("Contrary to Professor Kerr's view, this Note argues that courts should address the novel problem of computer searches by not treating it as a novel problem at all . . . ."), *with* LAWRENCE LESSIG, CODE: VERSION 2.0 at 164–65 (2006) (arguing that courts should "translate" their Fourth Amendment privacy protections to novel digital environments), *and* Kerr, *supra* note 48, at 280 (arguing it is necessary to look beyond the Fourth Amendment and to legislatures—rather than to courts—for creative, new solutions to problems posed by digital evidence collection).
[76] *See* Ghappour, *supra* note 37, at 1093, 1096.

web's relation to a new digital conception of the Fourth Amendment.[77] Because this Section focuses on the differences between the surface web and the dark web, it primarily focuses on the pre-2011 Internet. This date is important because, in 2011, Microsoft and Apple marketed cloud-based computing to the public,[78] which led to data shifting locations instead of remaining at a physically static URL. As the surface web becomes more like the dark web, this Note's observations about the latter can inform the former. However, an in-depth study of the effects of cloud computing is beyond this Note's scope.

In addition to some of the overlapping challenges discussed in the previous Section, searches on the dark web come with further hurtles. First, the dark web implicates international legal issues that the surface web does not. For example, imagine that someone hacked a bank located in Oklahoma and stole money through the surface web by obscuring the IP address and routing the money through other computers on the surface web. Although the location of the perpetrator might not be known, the location of the crime scene, Oklahoma, is. In contrast, the dark web obscures both the perpetrator and the "crime scene" because hosting data for the illicit websites are hidden as well. This means that both the perpetrator and the "crime scene" may or may not be out of the jurisdictional grip of the United States.[79] The dark web "is an enabler of cross-border, truly international crime where each of the major actors, evidence, and the proceeds of crime can all be in different jurisdictions."[80] This feature means that an investigation may require crossing jurisdictional and international boundaries, leading to potential conflicts of local laws.[81] One could employ the external conception of the Internet

---

[77] The only article that comes close is Wade Williams, *The Race for Privacy: Technological Evolution Outpacing Judicial Interpretations of the Fourth Amendment: Playpen, the Dark Web, and Governmental Hacking*, 45 FLA. ST. U. L. REV. 1211 (2018). However, this Note operates within the traditional conception of the Fourth Amendment.

[78] Keith D. Foote, *A Brief History of Cloud Computing*, DATAVERSITY (June 22, 2017), https://www.dataversity.net/brief-history-cloud-computing [https://perma.cc/XQU4-UYL6].

[79] *See* Tabachnick, *supra* note 11.

[80] Matthew Robert Shillito, *Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law*, 28 INFO. & COMM. TECH. L. 186, 206 (2019).

[81] To complicate this problem further, the Supreme Court held that the Fourth Amendment protects only those that have a "sufficient connection" or lawful presence in the United States, and based on this holding, digital, warrantless searches of foreigners' computers could technically occur constitutionally. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265, 271 (1990). The Court also examined whether the Fourth Amendment applies to a search and seizure of property located in a foreign country and owned by a nonresident alien. *Id.* at 261. The Court concluded that a nonresident alien with no intended attachment to the United States is not protected by the Fourth Amendment because that alien lacks "substantial connection" with the United States, and his property is located outside of the United States. *Id.* at 261, 271. Although this Note focuses on Rule 41(b) and conduct that necessitates a warrant, it notes that police operating not pursuant to a Rule 41(b) warrant could still legally gather digital evidence on U.S. citizens with no constitutional safeguards at all if that data is stored abroad. For example, to this day, the meaning of "lawful

and imagine that the crime took place along every node of the dark web, thus conferring jurisdiction along this path, but such a conception is limited in practice. It would be difficult to ascertain where each node was located *before* a warrant was issued and the internal/external distinction is itself problematic.[82]

Second, unlike the surface web, the traditional "exigent circumstances" categories that allow the police to investigate crime are futile when applied to the dark web. Functionally, there is no "plain view" because everything on the dark web is hidden. Moreover, the "third party doctrine" is of little use in the context of the dark web because Tor prevents police from identifying the server on which information is stored and therefore whom to subpoena. Furthermore, there is no way to prevent the destruction of evidence because the police have no way of knowing where the perpetrator is located. These limitations mean that, although these doctrines are not technically closed to investigators, they are, in essence, effectively closed. Thus, law enforcement's tools to investigate and stop dark web crime narrow even further.

Third, because the deep web—where the dark web can be found—is in flux, websites on it are dynamic in a way that websites on the surface web are not.[83] Illegal websites move locations every week, if not every day, "causing constant changes to the naming and address schemes."[84] Unlike information gathered two weeks ago from static websites on the surface web that end in *.com* or *.org* that may still be relevant today, information gathered from the dark web two weeks ago will likely no longer be relevant.[85] This short lifespan means that a judge's attempt to examine a URL involved in a criminal case would be futile because the URL leads nowhere.[86] More succinctly, although the surface web lacks geographical borders and exists in many places at once, the dark web seems to exist both everywhere and nowhere.

Fourth, even though the Fourth Amendment is grounded in privacy, the very idea of privacy is unworkable when applied to the dark web.

---

presence" in the United States when on a computer remains an open question of law because information about both U.S. citizens and foreigners is stored all over the world. *See* Vogt, *supra* note 44, at 113. Also, it is unclear whether the Fourth Amendment protects evidence obtained by the police when law enforcement mistakenly concludes that a suspect lacks Fourth Amendment rights, and how the Fourth Amendment works when an individual protected by the Fourth Amendment speaks with an individual who lacks such protection. *Id.*

[82] For a deeper discussion on this point, see *infra* Part III.

[83] *Q&A: The Deep Web, Anonymity, and Law Enforcement*, TREND MICRO (Sept. 10, 2015), https://www.trendmicro.com/vinfo/tr/security/news/cybercrime-and-digital-threats/qna-deep-web-anonymity-and-law-enforcement [https://perma.cc/NW2F-QZNQ].

[84] *Id.*

[85] *See id.*

[86] *Id.*

Individuals go to the dark web not just for privacy but for complete anonymity. With this in mind, they have exhibited a subjective expectation of privacy that society has recognized in some capacity, so any exploration of the dark web would therefore require a warrant.[87] However, in the case of a warrant and particularity (discussed in more detail below), law enforcement cannot know the location of the computer that investigators want to search, where to search within that computer, what they will find, or even to whom the computer belongs. These observations underlined the court's hesitation to grant a Rule 41 NIT warrant in *Carlson*:

> As there is no way to identify at the time the search warrant *was issued*, which computers, out of all the computers on planet earth might be used to log into [Playpen], the NIT warrant fails to particularly describe the place to be searched. . . . [T]he NIT warrant fails the particularity requirement because it does not identify which computers will be searched until the search is actually completed.[88]

Thus, a scholar is left with the questions: How should the dark web, and specifically the particularity requirement, be conceptualized, and how should Fourth Amendment doctrine address it? A detailed analysis of the particularity requirement in the digital age sheds light on a possible answer to such questions.

II. PARTICULARITY IN THE DIGITAL AGE

When drafting the Fourth Amendment, the Framers wished to prohibit the government from issuing general warrants. A general warrant "specifie[s] only an offense . . . and le[aves] to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched."[89] The particularity requirement, as interpreted by the U.S. Supreme Court in *Dalia v. United States*, requires three things to avoid amounting to an invalid general warrant: (1) "warrants must be issued by neutral, disinterested magistrates,"[90] (2) "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that

---

[87] For an example of similar reasoning as applied in the context of the surface web, see *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) ("Given the often sensitive and sometimes damning substance of [the defendant's] emails, we think it highly unlikely that [he] expected them to be made public, for people seldom unfurl their dirty laundry in plain view." (footnote omitted)). One could argue that no one has an expectation of privacy in illicit conduct, but the dark web is used for both illicit conduct and legal conduct. *See supra* notes 37–43 and accompanying text.

[88] United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, at *12 (D. Minn. Mar. 23, 2017), *report and recommendation adopted in part, rejected in part*, No. 16-317 (JRT/FLN), 2017 WL 3382309 (D. Minn. Aug. 7, 2017), *aff'd*, 769 F. App'x 400 (8th Cir. 2019).

[89] Steagald v. United States, 451 U.S. 204, 220 (1981).

[90] 441 U.S. 238, 255 (1979).

'the evidence sought will aid in a particular apprehension or conviction' for a particular offense,"[91] and (3) "'warrants *must particularly describe the "things to be seized,"' as well as the place to be searched*."[92] In *Dalia*, the Court found this requirement was satisfied when officers applied for a "court order authorizing the interception of oral communications occurring within petitioner's office" because "the exact location and dimensions of petitioner's office were set forth . . . and the extent of the search was restricted."[93] This requirement is designed to prevent "the wide-ranging exploratory searches the Framers intended to prohibit."[94]

Some courts found the particularity requirement was satisfied in the Playpen cases because the warrants "describe[] particular places to be searched—computers that have logged into [the website]—for which there was probable cause to search."[95] However, other courts found the particularity requirement was not satisfied because "the NIT warrant purports to be the description of the 'place to be searched,' but rather than describe a place, the Attachment describes a process by which the place [is] to be searched."[96]

---

[91] *Id.* (emphasis added) (quoting Warden v. Hayden, 387 U.S. 294, 307 (1967)).
[92] *Id.* (emphasis added) (quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)).
[93] *Id.* at 256 (citation omitted).
[94] Maryland v. Garrison, 480 U.S. 79, 84 (1987).
[95] *See* United States v. Darby, 190 F. Supp. 3d 520, 533 (E.D. Va. 2016); *see also, e.g.*, United States v. Broy, 209 F. Supp. 3d 1045, 1051 (C.D. Ill. 2016) (holding that even though the warrant "encompassed a large number of possible computers potentially located in a large number of districts," it did not fail the particularity requirement); United States v. Matish, 193 F. Supp. 3d 585, 608–09 (E.D. Va. 2016) (concluding "the NIT Warrant did not violate the Fourth Amendment's particularity requirement" because "there existed a fair probability that anyone accessing Playpen possessed the intent to view and trade child pornography"); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) (finding that the NIT warrant comported with the particularity requirement because it "explained who was subject to the search, what information the NIT would obtain, the time period during which the NIT would be used, and how it would be used, as well as bearing attachments describing the place to be searched and the information to be seized"); United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *5 (W.D. Wash. Jan. 28, 2016) ("Although the FBI may have anticipated tens of thousands of potential suspects as a result of deploying the NIT, that does not negate particularity, because it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network.").
[96] United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, at *11 (D. Minn. Mar. 23, 2017), *report and recommendation adopted in part, rejected in part*, No. 16-317 (JRT/FLN), 2017 WL 3382309 (D. Minn. Aug. 7, 2017), *aff'd*, 769 F. App'x 400 (8th Cir. 2019). Of the minority of courts that have suppressed evidence, most of them have been reversed. *See, e.g.*, *id.*; 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. Workman, 205 F. Supp. 3d 1256 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091 (N.D. Okla. Apr. 25, 2016); United States v. Levin, 186 F. Supp. 3d 26 (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017).

There is disagreement as to whether Rule 41(b)(6), which was adopted in response to debates over Playpen, complies with the particularity requirement outlined in *Dalia*. The warrants do not specifically fit within the confines of *Dalia* because the NIT warrants in the Playpen cases only described a process law enforcement would use to narrow down who would be searched.[97] They lacked the stated location to be searched as required by the third prong of *Dalia* because the location of Playpen's server and accessing computers was unknown *before* the warrants were issued.[98] This suggests that courts have considered the "place to be searched" too liberally because "computers that have logged into Playpen" are not a specific, physical location but a series of steps that an individual has taken. Therefore, under a traditional framework of the Fourth Amendment, Rule 41(b) NIT warrants should be void for lack of particularity and every defendant should be set free.

This issue speaks to a deeper disagreement over how to view the particularity requirement concerning the dark web, whether to do so from an internal perspective or an external one.[99] Like the internal/external perspectives within the search and seizure context articulated above, the conception of perspectives is important for the particularity requirement as well. When the internal/external perspectives are translated to the dark web, a few changes occur. First, the external perspective is seen more as a functionalist perspective, analyzing what the wires and the circuits do. Second, the internal perspective is thought of as more akin to the "traditional" Fourth Amendment particularity analysis, asking for an exact location or mailing address, as one would do in the nondigital world.

When thinking of the particularity analysis from these two perspectives, it becomes clear that most judges implicitly ascribed to the external perspective when they granted the Playpen warrant. For these judges, the "location" the warrant referred to was considered a process: logging onto the Playpen website. Judges viewed this as particular enough "because it would be highly unlikely that Website A would be stumbled upon accidentally, given the nature of the Tor network."[100] The judges were viewing the dark web from a functionalist perspective, analyzing the mechanisms of the anonymizing technology to allow for the substitution of a process for a true location. On the other hand, the judges who applied an internal perspective to particularity found the granted Playpen warrant unconstitutional because the *exact* location of the person to be searched was unknown before the warrant was issued.[101] Therefore, according to how the judges viewed

---

[97] *See, e.g.*, *Carlson*, 2017 WL 1535995, at *11.
[98] *See id.* at *12.
[99] This Note extends the application of Professor Kerr's discussion of the internal/external perspectives in the search and seizure context to the particularity context.
[100] *Michaud*, 2016 WL 337263, at *5.
[101] *See supra* note 96 and accompanying text.

the particularity requirement, either the defendant always won or the government did.

This dichotomist view of looking at NIT warrants would shut down a valuable tool to ferret out heinous crime taking place on the dark web or ensure that the government can trample over the defendant's rights. This enigma calls for a rethink of the doctrine undergirding particularity. Scholars such as Lawrence Lessig have advocated for courts to use "translation" when they apply old law to a new context,[102] as would be necessary when applying the Fourth Amendment to the Internet. Lessig suggests that when new circumstances arise that would have required a change in a legal text at the time of drafting, interpreters of the texts should "accommodate" changes to ensure "fidelity" to the text's original meaning.[103] Lessig argues this approach will ensure consistency across time when it comes to the application of the Fourth Amendment.[104]

Because the choice between the internal perspective and the external perspective decides the outcome of the warrant, this Note suggests a liminal approach, which would balance the government's interest in efficiently conducting criminal investigations against the privacy interests of the individual using the dark web by ensuring government investigation methods are necessary, limited in time and scope, and subject to a particularized process. Understanding that conceiving the digital world as either internal or external produces two different results, judges should apply the liminal approach—a distinct process—to ensure a more balanced view of the digital world. This is a more difficult conception of the dark web and perhaps not the most efficient for speedy judicial determinations. But balancing both individual liberties and continued government investigation is not a problem that should be speedily resolved. As Part III will show, using the liminal approach requires a rigorous process-based approach that is better positioned to address certain particularities in the digital world. The unique challenges the dark web presents require a new paradigm of the Fourth Amendment to be applied to digital investigations.

III. A FOURTH AMENDMENT FOR THE DARK WEB: THE LIMINAL APPROACH AND INDIVIDUAL RIGHTS

Courts holding NIT warrants valid and cementing the validity of such warrants in Rule 41(b)(6) signal the emergence of a new approach in navigating a digital Fourth Amendment. While Orin Kerr argues that courts should have a more limited role in constructing a digital Fourth Amendment,[105] this Note advocates for a more active role by courts. This Part is

---

[102] Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165, 1214 (1993).
[103] *Id.*
[104] *See id.* at 1232.
[105] *See* Kerr, *supra* note 48, at 280.

broken down into two sections. In Section A, it will become apparent that the process-based approach for which this Note advocates is warranted and constitutionally appropriate. However, in Section B, the Note will argue that additional protections are still necessary.

A. THE IMPLICATIONS OF VALIDATING RULE 41(B)(6) FOR A DIGITAL AGE

The addition of 41(b)(6) demonstrates that it is time for courts to explicitly recognize a process-based approach to the Fourth Amendment in the context of the dark web. When analyzing the decisions that allowed Rule 41 NIT warrants to be valid, it became comprehensible that the particularity requirement was relaxed and courts began to focus on the particular method of the search as opposed to the particular location to be searched.[106] Almost none of these courts outrightly acknowledged that they were relaxing the particularity requirement, but the truth of the matter is their rulings allowed a warrant for a location that was unknown at the time of issuance. This means, devoid of all artful misdirection, the courts were substituting procedures that they believed were needed in a digital context because the traditional procedures were failing them. In its entirety, the NIT warrant said:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL—upf45jv3bziuctml.onion—which will be located at the government facility in the Eastern District of Virginia.
>
> The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.[107]

---

[106] *See, e.g.*, United States v. Loera, 923 F.3d 907, 917 (10th Cir. 2019), *cert. denied*, 140 S. Ct. 417 (2019) ("Our electronic search precedents demonstrate a shift away from considering what digital location was searched and toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant.").

[107] United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, at *12 (D. Minn. Mar. 23, 2017), *report and recommendation adopted in part, rejected in part*, No. 16-317 (JRT/FLN), 2017 WL 3382309 (D. Minn. Aug. 7, 2017), *aff'd*, 769 F. App'x 400 (8th Cir. 2019).

The description is a process, not a location, but this Note argues that a description of a process still satisfies the particularity requirement in a digital conception of the Fourth Amendment.

In a situation like this, there is no "physical location" to be described.[108] The Internet can only be described as being in many different places (in the case of the surface web) or nowhere (in the case of the dark web).[109] Because this is the case, describing the process of a search is the closest one can get to an exact location. Put simply, if one was looking for a human on Earth, one could say they are everywhere on Earth. However, if you narrow the search to every human that bought a coffee at Starbucks on Thursday, purchased a new bed on Friday, and then ordered Chinese takeout on Sunday, the number would be significantly fewer. These criteria are not a location, but they are a description of the process that can be used to narrow the search. If the criteria narrow the search in the same way that an exact location would, then the function of the description of the process is remarkably similar to the listing of a specific location.[110] The open acknowledgement of this equivalence is what is needed to bring the Fourth Amendment into the digital age.

Moreover, the explicit passage of the amendment to Rule 41 to relax jurisdictional requirements for magistrate judges signifies a recognition of the challenges posed by the anonymity of the dark web. It signifies an understanding that the government's power must expand.[111] The courts' understanding of the limits of the traditional approach to the Fourth Amendment, and their attempts to fix it, directly challenge Professor Kerr's assertion that courts are not the best institutional actors to confront the digital age.[112] This relaxation of jurisdictional limitations directly addresses the problem of obscurity outlined above and is the most apparent way courts have addressed the rise of the digital age and the dark web. But a relaxation of jurisdictional limits must be balanced with protections for individual liberties—protections this Note lays out below.

B. RECOMMENDATIONS FOR A LIMINAL PERSPECTIVE TO PUSH FURTHER INTO A DIGITAL CONCEPTION OF THE FOURTH AMENDMENT

Recognizing that the government's power must expand due to reconceptualizing the Fourth Amendment for the digital age, one must also bulwark the shift with equal protection for individual rights. Therefore, since

---

[108] *See* Rustad, *supra* note 59, at 98 (explaining that Internet crimes do not involve the "traditional crime scene").
[109] *See supra* Part I.B.
[110] *Cf.* United States v. Spilotro, 800 F.2d 959, 964–65 (9th Cir. 1986) (citing cases discussing how the particularity requirement narrows the discretion of officers).
[111] For a discussion of how jurisdictional requirements constrained courts before the revision of Rule 41(b), see Ghappour, *supra* note 37, at 1124.
[112] *See* Kerr, *supra* note 48, at 280.

both the particularity requirement and the jurisdictional requirement for digital warrants have been relaxed under the external perspective, this Note advocates that protections for defendants need to be strengthened as well. One way to do this is by heightening the justification for a warrant.[113] Traditionally, a warrant is issued upon a showing of probable cause,[114] but depending on the type of electronic surveillance needed, some searches are authorized by subpoena, special court order, or notice to the individual.[115] There are a variety of proposals to increase the bite of probable cause or replace it altogether.[116] This Note proposes two replacements for the probable cause standard. Ultimately, it concludes that building off the two proposals is the best path forward in a digital conception of the Fourth Amendment and particularity.

1. Calls for Replacing the Justification Standard

Christopher Slobogin is a leading scholar in reconceptualizing the law of digital technology. In his seminal book, he criticized the traditional approach to the Fourth Amendment as relying too heavily on probable cause.[117] He advocates for a proportionality framework to replace the probable cause standard.[118] According to Slobogin, proportionality means the justification for the search must be roughly proportionate to its intrusiveness.[119] If the search is extremely intrusive, then the government needs a stronger justification to engage in that search. Slobogin suggests the use of data to measure the strength of the government's justification, specifically using hit rates as measured by the likelihood of success.[120] Such a proposal would do away with the balancing of reasonableness and encourage a more objective inquiry. This approach is used in "Canada, Germany, the European Court of Human Rights, India, Ireland, South Africa, and on occasion even in the United States."[121] In these countries and in a few cases in the

---

[113] *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299 (2004) (suggesting a probable cause requirement); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1592 (2004) (same).

[114] *See* U.S. CONST. amend. IV ("[N]o 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.").

[115] *Electronic Communications Privacy Act of 1986 (ECPA)*, BUREAU OF JUST. ASSISTANCE, OFF. OF JUST. PROGRAMS, U.S. DEP'T OF JUST., https://it.ojp.gov/privacyliberty/authorities/statutes/1285 [https://perma.cc/27G7-B6ML] (last visited April 12, 2021).

[116] *See infra* Part III.B.2.

[117] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 19 (2007).

[118] *Id.* at 21.

[119] *Id.*

[120] Christopher Slobogin, *Government Dragnets*, L. & CONTEMP. PROBS., 109, 139 (2010).

[121] Peter P. Swire, *Proportionality for High-Tech Searches*, 6 OHIO ST. J. CRIM. L. 751, 760 (2009) (quoting Vicki C. Jackson, *Being Proportional About Proportionality*, 21 CONST.

United States, "courts or tribunals invoke the basic concept of proportionality not only to review the propriety of sanctions, but also to measure the legality of a wide range of government conduct through some form of means-ends analyses."[122]

However, such a heightened standard would just replace one subjective test for another, as empirical analysis can be altered and modified to suit either a pro-plaintiff or pro-defendant interest.[123] Furthermore, Slobogin's focus on just a heightened standard of justification does not balance the scales of a new digital Fourth Amendment when compared to the expanded jurisdictional and relaxed particularity requirements outlined above. There must be more to ensure individual liberties. Even if Slobogin's test was substituted for the reasonableness of probable cause in the Playpen cases, the justification for the search—stopping a highly destructive ring of child pornographers—would be proportionate to the intrusiveness of the search. Therefore, a proportionality standard would result in no practical change because

> [w]hen investigating an Internet crime scene, the police almost always have probable cause whenever they have any suspicion at all due to the design of modern communications networks . . . . This important point has never before been recognized by legal scholars: the Internet is a hunch-free zone.[124]

This suggestion falls into a trap: a focus on justification standards or judicial review. Such a limited conception does not go far enough to safeguard individual liberties on the dark web:

> For other types of technologies, justification standards and judicial review continue to play an important rule, but they are blunt instruments of regulation, which provide an essential floor of protection from certain kinds of government overreach and abuse but do not do nearly enough to protect privacy and civil liberties. This is because a justification standard such as probable cause is a gatekeeping standard: once it is satisfied, it tends to say little about the scope, scale, or particularity of surveillance that is allowed.[125]

COMMENT. 803, 804 (2004) (reviewing DAVID M. BEATTY, THE ULTIMATE RULE OF LAW (2004))).

[122] *Id.*

[123] *See, e.g.*, *The Use—and Misuse—of Statistics: How and Why Numbers Are So Easily Manipulated*, KNOWLEDGE@WHARTON (Apr. 2, 2008), https://knowledge.wharton.upenn.edu/article/the-use-and-misuse-of-statistics-how-and-why-numbers-are-so-easily-manipulated/ [https://perma.cc/4T92-25D6].

[124] Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1515 (2010).

[125] Paul Ohm, *The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause*, *in* *THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW* 491–92 (David Gray & Stephen E. Henderson eds., 2017).

Although lower courts continue to focus on justification standards, the Supreme Court already ruled in *Berger v. New York* that it is a matter of constitutional law "that the judge's role is not completed once he or she finds probable cause for surveillance. Judges can and should impose other procedural safeguards tailored to address special problems with technological surveillance."[126] *Berger*, discussed further below, provides the route forward to safeguarding individual liberties in the digital age.

Professor Susan Freiwald considers the implications of *Berger* more fully and builds on Slobogin's justification standard. She considered such an approach in her article, *First Principles of Communication Privacy*.[127] In *Berger*, the Court invalidated New York's eavesdropping statute as too permissive under the Fourth Amendment.[128] The Court found the statute, which required judicial approval before conducting surveillance, invalid because there was a "heavier responsibility" to impose procedural protections for eavesdropping and wiretapping because they are so "broad in scope."[129] She advocates for the expansion of the test outlined in *Berger v. New York*, which limits well-established digital surveillance.[130] Under her test, whenever the police want to perform "hidden, intrusive, indiscriminate, and continuous" surveillance, they must satisfy the four requirements found in video surveillance cases: necessity, particularity, limited time, and minimization.[131] Professor Freiwald applies the approach from wiretapping to electronic communications like e-mail.[132] Going one step further, such an approach is also suitable for the dark web.

Because dark web investigations are "hidden, intrusive, indiscriminate, and continuous," additional requirements are needed to safeguard individual liberty.[133] Thus, whenever a warrant is sought under Rule 41(b), a court should inquire 1) if *necessity* is met by looking to whether agents seeking to use the NIT or malware have less intrusive means at their disposal; 2) if *particularity* is met by inquiring whether the court order authorizing the malware particularly describes the process of the search and the particular offense to which the surveillance is related; 3) if *limited time* is met by looking to whether the court order allows the NIT to go on longer than necessary to achieve its objective or—in any event—longer than thirty days, unless the order was extended; and 4) if *minimization* was met by observing

---

[126] *See id.* at 496 (analyzing Berger v. New York, 388 U.S. 41 (1967)).
[127] Susan Freiwald*, First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 5–6 (2007).
[128] *See Berger*, 388 U.S. at 55.
[129] *Id.* at 56.
[130] Freiwald, *supra* note 127, at 5–6.
[131] *Id.* at 15–16, 20 ("The test has courts focus where they should—on the nature of the surveillance, its power, its susceptibility to abuse, and the concomitant need for judicial intervention to keep it within appropriate bounds.").
[132] *See id.* at 6–8.
[133] *Id.* at 20.

whether the court order requires that the malware be conducted to minimize the capture of innocent bystanders.[134]

In the Playpen case, this new standard would have allowed for a warrant. First, the officers in the case attempted to infiltrate Playpen through undercover operations but had no luck, so deploying the NIT was a necessity.[135] Second, the agents particularly described the process they would use to narrow down only individuals that accessed the Playpen website.[136] Third, the warrant only authorized the NIT for the limited time of thirty days.[137] Fourth, the court order minimized the capture of innocent bystanders by requiring the monitoring of only those that had a username and password for Playpen and who logged onto the website.[138]

Necessity is what strengthens this standard the most. It could be the limiting principle for investigations on the dark web. Because there are other ways to gather suspects' information without invading their computers with an NIT,[139] law enforcement must try those methods before resorting to a Rule 41(b)(6) warrant. A time limit would also help safeguard individual liberty more than an average justification standard would. For example, under federal law, a wiretap approval is valid for only thirty days,[140] and approval to install and use a pen register is valid for only sixty days.[141] However, there is no federally required time limit on how long the police can access and investigate a computer.[142] These two tools, necessity and a time limit, would counteract the expansion of jurisdiction and the relaxation of the particularity requirement outlined above because a judge would

---

[134] Freiwald analyzes these four requirements with respect to video surveillance. *Id.* at 15–16. But this Note carries forward the application of the requirements to address concerns in investigations of the dark web.

[135] This information was garnered from personal conversations with prosecutors at the Department of Justice's Child Exploitation and Obscenity Section. Additionally, such undercover investigations are the standard for taking down anonymized forums. *See, e.g.*, Gemma Davies, *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers*, 84 J. CRIM. L. 407, 411 (2020) (explaining that undercover policing has "been used for some time in cyber investigations").

[136] See the warrant, reproduced in full, in United States v. Carlson, No. 16-317 (JRT/FLN), 2017 WL 1535995, at *12 (D. Minn. Mar. 23, 2017), *report and recommendation adopted in part, rejected in part*, No. 16-317 (JRT/FLN), 2017 WL 3382309 (D. Minn. Aug. 7, 2017), *aff'd*, 769 F. App'x 400 (8th Cir. 2019).

[137] *Id.*

[138] *Id.*

[139] *See supra* notes 45 and 46.

[140] 18 U.S.C. § 2518(5) (2018).

[141] *Id.* § 3123(c).

[142] *See The Police Seized Your Laptop—What Should You Do Next?*, DAVID PHILLIPS & PARTNERS (May 17, 2016), https://www.dpp-law.com/police-seized-your-laptop/ [https://perma.cc/Z5RF-UP5J] ("There is no set time limit relating to the seizure of any electrical devices, however, under the PACE act, your possessions must be made available as soon as they are no longer deemed necessary in the case. Or, if the charges against you are dropped, or if the case is resolved, the police will need to return your items.").

require not only procedural safeguards like a specific time and limited search scope but also the substantive safeguards of necessity.

2. Building on Slobogin's and Freiwald's Ideas

More is needed besides a new justification standard to align with the expansion of jurisdiction and the relaxation of the particularity requirement mandated by the modification to Rule 41. This Note advocates for a proposal that uses Slobogin's and Freiwald's new standards as only the beginning and not the end of an inquiry when it comes to the digital world. Under this approach—which this Note calls the liminal approach—a judge would engage in a two-part inquiry. First, she should concisely name the two perspectives at issue in the case—the internal perspective and the external perspective. The judge should then concisely state which perspective she is employing and why. This allows all parties to understand the reasoning behind her decision and to know the perception of the virtual world in which the parties are adjudicating. Because every court that used an internal perspective for the Playpen case was eventually overturned, the judge will most likely use an external perspective.[143] If the judge uses an external perspective, which favors the government, then she must ensure the "process" that the government has put forward sufficiently narrows down the digital location to be searched.[144] She would then proceed to the process-based justification standard that Freiwald advocates for. By naming the interests and delineating the digital world into its competing conceptions, the judge is providing a comprehensible framework of the legal system and reconceptualizing the particularity inquiry for a digital world.

To provide an example, suppose a police officer wants to investigate a dark-web forum that is full of inflammatory incitements to violence against a local high school. To do so, the officer wishes to deploy targeted malware to obtain the real-world locations of the site's users. The judge considering this officer's warrant application knows that the true locations of these users are currently unknown: although the investigation is being done in her jurisdiction, the users may rest outside of it. Thus, the judge should look at the particularity requirement from both the internal and external perspectives. According to the internal perspective, the internet is akin to reality and it is as if the dark web users are among a group of friends in an unknown location making threats against the school. Thus, the location of the users—

[143] *See* cases cited *supra* note 96.

[144] In the Playpen cases, the investigators were able to do this by narrowing down the process to capture "any user or administrator who logs into the TARGET WEBSITE by entering a *username and password*." *See e.g.*, United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *2 (W.D. Wash. Jan. 28, 2016) (emphasis added). By requiring a username and password to be entered, the process was sufficiently narrow to define the location. *Id.* at *4–*5. It is conceivable that if the warrant had not required users to enter their username and password, but instead merely load the page, then the process, in that hypothetical, would not have been sufficiently particular.

where they are currently in the world—is also unknown, and the particularity requirement is not met. From the external perspective, the warrant application has proposed that the process of targeting all users who enter their username and password on the dark web site is sufficiently particularized. When these two conceptions are stated, the judge must then decide which perspective she is using. If she uses the external perspective, as most judges did in the Playpen case, she must decide if the "process" proposed sufficiently narrows down the pool of targeted individuals. Here, unlike in the Playpen case, that might not have occurred because the proposed process could capture individuals logging on to the dark website who did not engage in the inflammatory incitements of violence.

Nevertheless, if the judge finds the "process" particular enough, the judge must next consider it within her power to authorize a warrant for this search, regardless of jurisdictional requirements if, and only if, all other routes of investigation have already been attempted. Such a decision employs the liminal approach because it conceives of the dark web as a physical space that is about to be invaded and needs to be safeguarded (the internal approach), while also recognizing that the government has outlined a process, conducted through the least restrictive means, to obtain technical code through wires that run through her jurisdiction (the external approach). By requiring a necessity showing, the judge would be basing her decision on the outcomes of investigations based in the digital world, not on outdated conceptions of the Fourth Amendment developed in relation to the physical world.

In closing, it is important to note this author's concern that this process-based idea is still not enough to fully protect individual liberties. However, Fourth Amendment precedent focused on the physical world had nearly 230 years to develop and protect the individual from unreasonable search and seizure.[145] Hopefully, in time, additional precedents protecting individual liberties in the digital age will be created to buttress the process-based approach described above. One option among many could be to create courts that specialize in dark web and anonymized warrants, much like the Foreign Intelligence Surveillance Court specializes in "approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes."[146] However, it is beyond the scope of this Note to fully flesh out a complete system of additional Fourth Amendment protections for the digital world.

---

[145] The Fourth Amendment was ratified in 1791.

[146] *About the Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTEL. SURVEILLANCE CT., https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court [https://perma.cc/SVV6-5NRY] (last visited April 12, 2021).

CONCLUSION

The dark web is complicated. It provides a haven against tyrannical governments but also provides a haven for individuals to explore their depravity. It has developed for years with little legal oversight and little application of the Fourth Amendment within its encrypted space. As more of our lives transition online, it is important to analyze *all* aspects of the Internet—not just the surface web, which makes up only a small portion of the Internet. The dark web is likely here to stay, so it is time to take a hard look at legal mechanisms and allow the dark web to expand while also constraining its darker impulses. As with much of this Note, such a contradiction is one that must be carefully teased apart to successfully reveal the connection between expanding and constraining this new frontier.

Although the dark web presents even more challenges than does the surface web for a digital conception of the Fourth Amendment, this Note focuses on delving into the implications of courts' rulings on a Rule 41(b) warrant for a digital conception of the Fourth Amendment. It identifies the courts' relaxation of the particularity requirement and jurisdictional standards as direct responses to the challenges the dark web poses. However, because there has been no equal increase in individual protection under a digital conception of the Fourth Amendment, this Note presents only an initial solution to this problem.