Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 29 *XXIX*
Number 4

Article 6

2019

The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching

Denae Kassotis
dkassotis@fordham.edu

The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching

Cover Page Footnote
J.D. Candidate, Fordham University School of Law, 2019; B.A., History, University of Delaware, 2016. This Note was prepared with the assistance of Professor Olivier Sylvain who served as my faculty adviser on the project. I would also like to thank John Bradshaw and Elias Wright for their input and edits. Lastly, I would like to thank my father, John Kassotis, for his suggestions and constant mentorship.

The Fourth Amendment and Technological Exceptionalism After *Carpenter*: A Case Study on Hash-Value Matching

Denae Kassotis*

The Fourth Amendment has long served as a barrier between the police and the people; ensuring the government acts reasonably in combating crime. Fourth Amendment jurisprudence is more dynamic than other constitutional guarantees, and has undergone periodic shifts to account for technological and cultural changes. The Supreme Court's 2018 decision in United States v. Carpenter marks the most recent jurisprudential shift, as the Court departed from the well-settled reasonable expectation of privacy test to account for a new technology (CSLI records). This Note examines Carpenter's impact on future Fourth Amendment cases, using another novel surveillance technique, hash-value matching, as a case study. Hash-value matching is a binary authentication method that can scan billions of digital communications in seconds for evidence of contraband.

* J.D. Candidate, Fordham University School of Law, 2019; B.A., History, University of Delaware, 2016. This Note was prepared with the assistance of Professor Olivier Sylvain who served as my faculty adviser on the project. I would also like to thank John Bradshaw and Elias Wright for their input and edits. Lastly, I would like to thank my father, John Kassotis, for his suggestions and constant mentorship.

INTRODUCTION

Have you ever wondered how your email account verifies that you have entered the correct password when you attempt to log-in? Websites that require a user to log-in with a password keep a repository of hash-values corresponding to passwords that unlock specific user's accounts.[1] When a user first creates their password, the alphanumeric string they enter is run through a hash algorithm, converting it into a shortened output with a fixed length.[2] This output, known as the password's hash-value, is then saved by the website.[3] When a user later attempts to log-in with the same input, the input will again be run through the hash-algorithm to create a hash-value.[4] If the hash-value for the attempted log-in matches the stored hash-value, corresponding to the password initially entered, the user will be allowed to proceed into the account.[5] Moreover, since websites store password's hash-values, which cannot be converted back to the passwords they correspond to, even if their repository of hashes was hacked, a hacker would not be able to retrieve the desired passwords.[6]

The process used to verify passwords is called data-exposure.[7] Data-exposure refers to a model where an entity keeps a repository of hash-values corresponding to known inputs (such as correct passwords), and compares unknown inputs (such as attempted passwords) against the repository to "expose" a match.[8] If an unknown input matches a known hash-value, it is certain that the

---

1 *Understanding Password Authentication & Password Cracking*, WORDFENCE, https://www.wordfence.com/learn/how-passwords-work-and-cracking-passwords/ [https://perma.cc/9GUQ-EV9E] (last updated June 25, 2018).

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

6 *See id.*

7 *Cf.* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash,* 119 HARV. L. REV. 38, 43 (2005) (defining data exposure as matching an unknown set of hash-values against a known hash list to reveal particular files.); *see also infra* Introduction.

8 *Id.*

unknown input is the same as the input that created the known hash-value.[9]

Safe password storage is one of many innocuous uses of data exposure. For example, law enforcement can compare a suspect's hard-drive against a customized hash-list to look for files stolen during an intrusion, or for pirated software not yet released to the public.[10] These examples refer to a targeted government search of lawfully acquired private property for digital contraband. But, law enforcement is not the only entity with access to hashing software. In fact, conglomerates like Microsoft hash every file sent through their network for evidence of child pornography.[11] Social giants such as Facebook, Twitter, Microsoft, and YouTube hash user content to thwart the distribution of terrorist content and curtail protest activity.[12] ISPs like AT&T have discussed hashing user data to identify copyright infringing music or movies shared among friends.[13] Moreover, private companies are encouraged, both by law and social norms, to turn over evidence of hash-matches to law enforcement. Although it is in society's best interest for law enforcement to receive much of this evidence, where is the line drawn? Furthermore, is the Fourth Amendment triggered when private actors systematically share evidence with the government?

---

9 *Id.* at 40.

10 *Id.* at 43.

11 *See* United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *3 (S.D. Tex. Apr. 13, 2017).

12 Kalev Leetaru, *Can We Finally Stop Terrorists from Exploiting Social Media?*, FORBES (Oct. 9, 2018, 7:01 PM), https://www.forbes.com/sites/kalevleetaru/2018/10/09/can-we-finally-stop-terrorists-from-exploiting-social-media/#7ce5faae6d80 [https://perma.cc/8SNY-R9WL]; *Facebook, Microsoft, Twitter, and YouTube Provide Update on Global Internet Forum to Counter Terrorism*, MICROSOFT CORP. BLOGS (Dec. 4, 2017), https://blogs.microsoft.com/on-the-issues/2017/12/04/facebook-microsoft-twitter-and-youtube-provide-update-on-global-internet-forum-to-counter-terrorism/ [https://perma.cc/A6BS-24XM].

13 *See* Brad Stone, *AT&T and Other I.S.P.'s May Be Getting Ready to Filter*, N.Y. TIMES: BITS BLOG (Jan. 8, 2008, 7:07 PM), https://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/ [https://perma.cc/E676-Q6D2]; *see, e.g.*, *In re* United States of America's Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1152 (W.D. Wash. 2011).

This Note proceeds in three Parts. It assesses the impact of *United States v. Carpenter* on Fourth Amendment rights by exploring the admissibility of hash-match evidence of child pornographic images, that are intercepted by a private actor and shared with the government via statutory mandate. Part I of this Note introduces hash-value matching technology and explores the effect of hashing, as well as other information age technologies, on information privacy. Next, Part I discusses the regulatory shortcomings of the federal law's ability to govern information privacy. Finally, it analyzes the private and binary search doctrines and discusses the state of Fourth Amendment doctrine before and after *Carpenter*.

Part II further unpacks the *Carpenter* decision and its impact on a Court reviewing an "exceptional" technology under the Fourth Amendment. Part II also proposes a new framework to determine if a technology is exceptional, meaning that technology should not be analogized to previous technologies of its kind. In determining technological exceptionalism, this Note proposes an inquiry into whether a technology is fundamentally different from others of its kind, and whether the technology is "much less costly" for the government to employ. Moreover, this Note proposes that if a technology meets the definition of "exceptional," it causes a rights-shift. A rights-shift occurs when the low cost of a new surveillance method allows the government to engage in a surveillance activity it was once precluded from. A rights-shift disrupts the balance struck by the Fourth Amendment between law enforcement and citizens. This Note proposes that in response to an unbalanced Fourth Amendment, courts should follow Justice Robert's approach in *Riley* and *Carpenter* and holistically assess the technology at issue. Further, in the rare circumstance that a technology is deemed exceptional, courts should look at the totality of the circumstances in assessing the diminution in privacy caused by the technology, and avoid rigidly applying the reasonable expectation of privacy test. Finally, Part III assesses the Fourth Amendment implications of hash-value matching pursuant to the framework proposed in Part II.

I. OVERVIEW OF HASH-VALUE MATCHING, INTERNET GOVERNANCE, AND INFORMATION PRIVACY

A. Hash-Value Matching

Hashing is a common forensic technique used to analyze digital images taken from a computer.[14] It is "the process of taking an input data string from an electronic [file] and using a mathematical function to generate a (usually smaller) output string."[15] The output string, called the hash-value,[16] is a "digital fingerprint" shared by any duplicate of the input data string.[17] Any two iterations of the same file will, with over ninety-nine percent accuracy, produce the same hash-value.[18] Thus, hash-values are uniquely associated with the input data, such that, "if an unknown file has a hash-value identical to that of another known file, then [it is clear] that the first file is the same as the second."[19] One of the advantages of hashing software is the ability to scan a large number of electronic files for their hash-values in very little time, and, do so without exposing the underlying image corresponding to the hash to third-party viewers.[20]

The cryptographic, or "one-way," hash algorithm, referred to in this Note, is impossible to reverse—that is, to turn the hash-value

---

[14] *See* United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *1 (E.D. Ky. June 23, 2017).

[15] *Id.* (citing Salgado, *supra* note 8, at 38–39).

[16] The terms "hash" and "hash-value" are interchangeable and will be used interchangeably throughout this paper. *Forensic Use of Hash Values and Associated Hash Algorithms*, NETH. FORENSIC INST. 2 (Jan. 2018), https://www.forensischinstituut.nl/binaries/nfi/documenten/publicaties/2018/02/13/vakbijlage-forensisch-gebruik-van-bestandskenmerken-en-bijbehorende-hashalgoritmen/Supplement-hashes-v2018_01a_English.pdf [https://perma.cc/2M6F-T33E].

[17] *Miller*, 2017 WL 2705963, at *1. With respect to images and videos, hashing software breaks them down into bits of data, and assigns that data alphanumeric values based on the image's hue gradient. The resulting string of numbers is the image's hash-value. Since a hash-value is derived from each "bit" of data, and its placement relative to other bits, it is intimately associated with the image. *See* NETH. FORENSIC INST., *supra* note 16, at 2.

[18] United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *1 (S.D. Tex. Apr. 13, 2017).

[19] *Miller*, 2017 WL 2705963, at *1.

[20] *Reddick*, 2017 WL 1353803, at *2.

back into the underlying image it identifies.[21] Moreover, it is practically impossible[22] to find two files that have different content but the same hash value.[23]

1. Detecting Child Pornography

Hashing has an array of forensic purposes, including the identification, verification, and authentication of data.[24] One such purpose, known as "data exposure" or hash-value matching,[25] is the process of matching a hash-set[26] associated with an individual's files against a known hash set to reveal particular files.[27] Hash-value matching can accurately and expeditiously identify whether a computer contains known digital contraband.[28] This Note specifically addresses the use of hash-value matching to determine whether a suspect's computer contains child pornographic images, and the subsequent use of such hash evidence at a criminal trial.

The advent of the internet provided a new means for trafficking child pornography.[29] In response to the ever-increasing use of internet communication, Congress created a statutory scheme to identify digital files containing child pornography, which conferred

---

21 NETH. FORENSIC INST., *supra* note 16, at 3.

22 In this context, "practically impossible" can be read as "even when all the computing power of the world could be used simultaneously, it is still impossible." *Id.* at 3 n.4.

23 *Id.* at 3.

24 *See generally* Salgado, *supra* note 8, at 43.

25 Hash-value matching is the process of matching a media hash set against a known hash set to reveal particular files. This process is also known as data exposure. *Id.* For purposes of this Note, which focuses on the use of hash-values, the aforementioned process is generally referred to as "hashing." *See id.*

26 In this context, a "hash-set" refers colloquially to the list of hash-values associated with an individual's files. *See* NETH. FORENSIC INST., *supra* note 16, at 2.

27 *See id.*

28 *See id.*

29 Alexandra L. Mitter, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 N.Y.U. ANN. SURV. AM. L. 235, 241 (2011) ("Before the advent of the Internet, production and reproduction of pornographic images involving children were extremely difficult and expensive, and the sale and distribution of those images were similarly risky endeavors.").

broad investigative powers on federal and local government.[30] Congress's response was swift and effective, in part because its legislation capitalized on the unique position of electronic communication service providers ("ECSPs"), specifically, Internet Service Providers ("ISPs").[31] Although this scheme has been efficient in reducing the spread of child pornography, it implicates Fourth Amendment and information privacy concerns for every individual who communicates digitally.[32] The following Section discusses hashing's central role in the statutory framework curtailing the spread of digital contraband.[33]

2. The Reporting Dynamic Between ECSPs and Law Enforcement

Pursuant to the Crime Prevention Act of 1990, "[a] person who, while engaged in a professional capacity . . . learns of facts that give reason to suspect that a child has suffered an incident of child abuse . . . and fails to make a timely report" can face a fine or imprisonment.[34] Further, the PROTECT ("Providing Resources, Officers, and Technology to Eradicate Cyber Threats") Our Children Act provides that any electronic communication service ("ECS")[35] or remote computing service ("RCS") provider that

---

[30] *See* 18 U.S.C. § 2258A(a) (2012).

[31] *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 5 U. ILL. L. REV. 1417 (2009); *infra* Part I.A.3.

[32] *See infra* Part III. Per a 2018 study, there will be over 3.8 billion email users before the start of 2019. That is over half of the world's population. Heinz Tschabitscher, *How Many Email Users are There?*, LIFEWIRE, https://www.lifewire.com/how-many-email-users-are-there-1171213 [https://perma.cc/SF3K-NZE3] (last updated Dec. 16, 2018).

[33] *See, e.g.*, Child Protection and Obscenity Enforcement Act of 1988 [CPOEA], Pub. L. No. 100-690, 102 Stat. 4485 (codified as amended at 18 U.S.C. § 2251 (2006)); Child Pornography Prevention Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009 (codified in scattered sections of Titles 18 and 42 U.S.C.); PROTECT Act of 2003, Pub. L. No. 108-21, 117 Stat. 650, 676–86 (codified in scattered sections of Title 18 U.S.C.) ("Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today").

[34] 42 U.S.C. § 13031 (2012); *see, e.g.*, United States v. Stratton, 229 F. Supp. 3d 1230, 1233 (D. Kan. 2017).

[35] "'[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2012).

obtains actual knowledge of an image depicting child pornography is required to provide a report to the National Center for Missing and Exploited Children's ("NCMEC") CyberTipline[36] "as soon as reasonably possible."[37]

Moreover, "[m]any [ECS] providers, desiring to avoid any reputation for aiding those who possess or transmit child pornography, use [hashing software] to scan files that customers upload through the service providers' browsers, applications, or cloud storage facilities."[38] Major ECSPs, such as Microsoft, compare hash-values generated from user content that correspond to confirmed images of child pornography.[39] Hash-values saved in the NCMEC repository or similar database are compared with the hash-values of files transmitted or stored on an ECSP's server by its automated hashing software.[40] Pursuant to the PROTECT Act, if a provider gets a match, the provider must refer the files, along with the sender's subscriber information, to NCMEC.[41] NCMEC operates a database that serves as the central repository of hash-vales for confirmed images depicting child pornography.[42]

---

[36] NCMEC launched its CyberTipline in 1998 to help battle the sexual exploitation of children by providing the public and ECS providers with the ability to report online instances of exploitation. *CyberTipline*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., www.missingkids.com/gethelpnow/cybertipline [https://perma.cc/4P3P-VZDW] (last visited Jan. 30, 2019).

[37] 18 U.S.C. § 2258A(a)(1) (2012).

[38] United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *2 (S.D. Tex. Apr. 13, 2017). "Google, has been using its proprietary hashing technology since 2008 to identify 'confirmed child sexual abuse images.' After an image of child sexual abuse is viewed 'by at least one Google employee,' the image 'is given a digital fingerprint (hash)' and is added to Google's repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256." United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *1 (E.D. Ky. June 23, 2017). "AOL's automated filter works by identifying the hash values of images attached to emails sent through its mail servers. Those values are then compared to the hash values of images that AOL employees have viewed previously and deemed child pornography. Any email containing an image with a matching hash value is automatically weeded out." United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016).

[39] *Reddick*, 2017 WL 1353803 at *2.

[40] *Id.*

[41] *See id*. at *3; 18 U.S.C. § 2258(A).

[42] *Reddick*, 2017 WL 1353803, at *2.

After an ECSP submits a report to the CyberTipline, NCMEC, viewing the hash-value only, generates its own report.[43] NCMEC then conducts an initial investigation, limited to confirming the hash-value match and identifying the location of the internet user whose equipment uploaded the matching file.[44] Finally, NCMEC forwards the report to the law enforcement agency with jurisdiction over the internet user.[45] Further, the internal policies of most ECSP's regarding the use of proprietary hashing software contemplate that a human employee will confirm that the image depicts child pornography before a report is submitted to NCMEC.[46]

Litigation arising from this dynamic principally consists of criminal defendants arguing that this scheme violates their Fourth Amendment rights.[47] However, at least before *Carpenter*, the intermediary role of ECSPs, results in the dismissal of almost all Fourth Amendment challenges. The following Subsection discusses issues concerning ISPs as information intermediaries.

---

43 *See id*. at *3.

44 *See id.*

45 *See id.*

46 *See Partnering to Help Curb Spread of Online Terrorist Content,* FACEBOOK NEWSROOM (Dec. 5, 2016), https://newsroom.fb.com /news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/ [https://perma.cc/KA8E-6J6U] (describing Facebook's use of hashing software to remove violent terrorist imagery and its policy to review material that matches a hash-value known to depict terrorist content before automatically removing the material); *supra* note 38 and accompanying text. For example, Google maintains a repository of apparent child pornography, as defined by 18 U.S.C. § 2256, which consists of images that have been determined to depict child pornography by "at least one Google employee." When Google encounters a hash that matches a hash of a known child sexual abuse image, it undertakes a manual human review to confirm the image contains child pornography. The typical process looks like Google's proprietary hashing software. *See* United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *1 (E.D. Ky. June 23, 2017).

47 *See e.g.*, *Miller*, 2017 WL 2705963.

3. The Crucial Role of an ISP in Obtaining Hash Evidence

An ISP,[48] subject to the reporting requirements of the PROTECT Our Children Act,[49] has a unique and crucial role in routing its user's communications to the rest of the world.[50] An ISP owns the point on the network between a user's computer and the rest of the internet—the only point through which all the user's communications must pass.[51] This chokepoint allows ISPs to engage in large scale surveillance of its users, accessing more information than any other type of electronic service provider—even Google.[52] Since ISPs are the "gateway," or first-step, to the

---

[48] An internet service provider is a "company that provides internet connections and services to individuals and organizations. In addition to providing access to the Internet, ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page." *Internet Service Provider*, ENCYC. BRITANNICA, https://www.britannica.com/technology/Internet-service-provider [https://perma.cc/LQ26-5AA6] (last visited Apr. 15, 2019).

[49] ISPs meet the statutory definition of an ECSP under the PROTECT Our Children Act. 18 U.S.C. §2258(a) (2012) (defining "reporting requirements of providers.") Courts have struggled to correctly classify different electronic communications providers. *See, e.g.*, United States v. Richardson, 607 F.3d 357, 360 (4th Cir. 2010) (labeling AOL an internet service provider). However, the text and spirit of the PROTECT Act and judicial precedent indicate that ISPs are the exact entity Congress intended to subject to reporting requirements. In general, due to network design, a user's communication must pass through a "privileged network bottleneck" controlled by his ISP to reach other internet users or sites. Put differently, "a user cannot say anything to Google without saying it first to his ISP, and an ISP can [] hear everything a user says to other websites like Facebook." Ohm, *supra* note 31, at 1420. Thus, ISPs have greater access to electronically transmitted communications than any other electronic service provider—even Google. *See id.* Ohm defines an ISP as a "telecommunications compan[y] that route[s] communications to and from Internet-connected computers." *Id.* at 1420 n.1. This definition of ISP falls squarely within the statutory definition of an ECS, i.e., "any service which provides to users thereof the ability to send and receive wire or electronic communications." 18 U.S.C. § 2510(15) (2012).

[50] Ohm, *supra* note 31, at 1423.

[51] *Id.*

[52] *Id.* at 1420. "Likewise, the ISP can scrutinize communications sent to almost all of Google's other services. Every time a user adds an appointment to his Google Calendar, sends or receives an e-mail message through Gmail, reads blogs using Google Reader, edits a word processing document in Google Docs, or views a video in Google-owned YouTube, his computer sends copies of his messages, requests, and behavior first through his ISP." *Id.* at 1440.

Internet, "almost any communication sent to anybody online" is accessible first by an ISP.[53] Further, by imposing reporting obligations on ISPs and immunizing them from suit, Congress both recognized and ratified their unique enforcement role.[54]

In the early days of the internet, ISPs conducted broad automated monitoring of their user's communications for business purposes, such as gauging the health of the network, detecting spam, and policing bandwidth.[55] Such automated monitoring was relatively non-invasive, since ISPs preserved privacy by "keeping a shallow, limited view" of user's communications.[56]

However, sparse legal constraints on ISPs, incentive to monetize user data, and technological advances led to a shift in ISP monitoring behavior in the 2000s.[57] The combination of these factors gave ISPs the motive and the means to deeply scrutinize their user's communications.[58] First, after Google demonstrated the efficacy of monetizing user behavior by displaying advertisements targeted to user's search queries, ISPs followed suit.[59] Next, before the early 2000s, network monitoring was constrained by the relative slowness of computers and technological limitations on

---

[53] *Id.* at 1438. "ISPs can view [user activity] across the Internet landscape, seeing everything we do regardless of destination or application." Additionally, an ISP can view its user's activities deeply, "because packet sniffers can store everything." *Id.*

[54] 18 U.S.C. §§ 2258(A)–2258(B) (2012). An ECSP who obtains actual knowledge of child abuse must report it to NCMEC. 18 U.S.C. § 2258(A). No civil claim or criminal charge may be brought against an ECSP arising from its reporting responsibilities in any Federal or State court. 18 U.S.C. § 2258(B).

[55] Ohm, *supra* note 31, at 1424.

[56] *Id.*

[57] *See id.* at 1425, 1427, 1432. Google, by displaying advertisements matching user's recent search inquiries, was the first ECSP to successfully monetize user's browsing behavior. Other ECSPs have attempted to follow suit and capitalize on user's behavioral data, a phenomenon known as "Google envy." *Id.* at 1426.

[58] *Id.* at 1432.

[59] *Id.* at 1426. Arguably, ISPs were forced to find an additional source of revenue in response to novel internet applications that required large amounts of bandwidth and burdened existing network infrastructure. ISPs had to invest significant capital in their infrastructure to support increased bandwidth, but customers were unwilling to pay astronomical monthly fees to fund the increase. *Id.* at 1425–26.

monitoring hardware.[60] Put differently, ISPs lacked the computing horsepower to swiftly capture and analyze communications sent across their networks.[61] Professor Ohm[62] analogizes the limitation on pre-2000 network monitoring to a single police officer monitoring traffic on the side of a country road.[63] How thoroughly the officer can scan the passing cars depends on two metrics: how many cars drive by in a fixed time-period, and how quickly the officer can scan each car.[64] The first metric, the volume of traffic, is akin to how many communications pass through a network (bandwidth).[65] The second, the officer's efficiency, represents the relative capabilities of network monitoring tools.[66]

Post-2000, the horsepower of internet monitoring software (the officer's efficiency) increased at a quicker rate than the network's bandwidth (the volume of traffic).[67] Thus, a former technological constraint on an ISP's ability to monitor—the relative slowness of monitoring software—is no longer in play.[68] In contrast to the single police officer alongside a country road, the post-2000 metaphor would involve several police officers, trained to work at optimal efficiency, monitoring traffic with the help of radar guns.[69] Moreover, although the country road is replaced by a busy highway, the relative increase in the officers' capabilities is greater than the increase in traffic.[70]

---

60 *Id.* at 1427. Lawrence Lessig, a Harvard professor focusing on internet governance and constitutional law, identified four regulators of online conduct as: markets, norms, law, and technology. *Id.*

61 *Id.* at 1428.

62 Paul Ohm is the Associate Dean for Academic Affairs at Georgetown Law. He specializes in information privacy, computer crime law, intellectual property, and criminal procedure. *Paul Ohm*, GEO. LAW, https://www.law.georgetown.edu/faculty/paul-ohm/ [https://perma.cc/56E9-WT88] (last visited Jan. 30, 2019).

63 Ohm, *supra* note 31, at 1428.

64 *See id.*

65 *See id.*

66 *See id.* at 1430.

67 *Cf. id.* at 1430–31.

68 *Cf. id.*

69 *See id.* at 1428–31.

70 *Id.* at 1427–28.

Finally, lawmakers swiftly recognized the unique and important role of ISPs in combating crime.[71] Thus, following pressure from law enforcement agencies, Congress vested ISPs with certain responsibilities and immunities to assist law enforcement.[72] Relatedly, there are sparse federal protections over private information held by ISPs and other third-parties.[73] The resulting framework grants ISP's the broad ability to monitor network traffic and gather user information. Moreover, it affords law enforcement easy access to the stored consumer-data.[74]

4. Federal Framework Regulating Information Privacy

The United States lacks a comprehensive data security law regulating the collection and use of personal data on the federal level.[75] Instead, states and independent agencies are tasked with regulating the collection and use of personal data.[76] The result is a non-standardized, "patchwork" system of incongruent laws that cannot efficiently regulate consumer privacy.[77]

Moreover, there is no federal law governing mass collection of private information.[78] The modest federal protections on consumer data come from the Federal Trade Commission ("FTC"), which has overseen privacy regulations since the 1970s.[79] Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), the FTC is authorized to "prohibit[] unfair or deceptive acts in the

---

71 *Id.* at 1426–27.

72 *See, e.g.*, 18 U.S.C. § 2258(A) (2012).

73 *See generally* Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. L. (Oct. 1, 2018), https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1 [https://perma.cc/F66C-ZF7J].

74 *See generally id.*

75 *Id.*

76 *Id.*

77 *See generally id.*

78 *Id.*

79 Cheryl Wang, *Information Privacy and Data Security Laws: An Ineffective Regulatory Framework*, COLUM. UNDERGRADUATE L. REV. (Oct. 31, 2017), http://blogs.cuit.columbia.edu/culr/2017/10/31/information-privacy-and-data-security-laws-an-inefficient-regulatory-framework/#_ftn3 [https://perma.cc/F2HC-6KYZ].

marketplace"—which allows it modest regulatory power over data collection practices.[80] However, the FTC's enforcement authority is limited, exemplified by its high profile action involving Levnovo, one of the world's largest personal computer ("PC") manufacturers, and Superfish, a browser-based advertising company, in 2017.[81]

Between 2014 and 2015, Lenovo pre-installed Superfish's ad-injecting software (called "Visual Discovery") on all its computers.[82] This "man-in-the-middle" technique allowed Superfish access to user's sensitive data—including social security numbers, financial account information, login information, and emails—by establishing Visual Discovery as a local proxy between a user's PC and the websites they visited.[83] Lenovo and Superfish made profited off of this scheme.[84] In response, the FTC charged Lenovo with deceptively failing to "disclose adequately, that VisualDiscovery would act as a man-in-the-middle" and for unfairly preinstalling the software without notice to consumers.[85] It thus follows that, if another company disclosed its "man-in-the-middle" software to consumers, such an action would likely be outside the regulatory authority of the FTC.[86] Moreover, exemplified by the FTC's "roundabout" way of holding Lenovo liable, it can only regulate to prohibit market inequities—it cannot regulate the mass collection of data in the first instance.[87] The FTC's limited authority is the major federal regulation concerning data privacy; leaving most mass data collection completely unchecked.[88]

---

80 *Privacy and Data Security Update (2016)*, FED. TRADE COMM'N (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016#how [https://perma.cc/Z6X4-DHDT].

81 *See* Wang, *supra* note 79.

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id*.

86 *See id.*

87 *See generally id.*

88 *See, e.g.*, 15 U.S.C. § 45 (2012) (authorizing the FTC to declare unlawful "unfair" or "deceptive" acts affecting interstate commerce.); *see also* FED. TRADE COMM'N, *FTC Releases 2018 Privacy and Data Security Update*, https://www.ftc.gov/news-events/press-releases/2019/03/ftc-releases-2018-

Additionally, in early 2017, the Trump administration signed a Congressional resolution repealing an Obama-FCC rule that would have required ISPs obtain explicit consumer permission before sharing or selling sensitive information.[89] The resolution allows ISPs, which are treated differently than other communication providers, to collect, store, share, and sell certain types of data, including location information, browsing history, and app-usage data, without a user's consent.[90] Thus, ISPs can, and do, store massive amounts of user information for a variety of business purposes, with essentially no legal hurdles.[91]

In addition to sparse regulation concerning *monitoring* and *storing* consumer data, federal law does not effectively prevent the disclosure of stored information. The primary statute regulating disclosure of electronically stored information is the Stored Communications Act ("SCA").[92] The SCA was enacted in 1986, in response to the judicially crafted third-party doctrine,[93] in an attempt to protect individuals' private communications held in electronic storage by ECSPs.[94] Congress tailored the SCA to electronic communications sent via and stored by third-parties by establishing that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in

privacy-data-security-update [https://perma.cc/X39X-THSD] (Mar. 15, 2019) ("[t]he Federal Trade Commission [is] the nation's primary privacy and data security enforcer.")

89 Kaveh Waddell, *Encryption Won't Stop Your Internet Provider from Spying on You*, ATLANTIC (Mar. 29, 2017), https://www.theatlantic.com/technology/archive/2017/03/encryption-wont-stop-your-internet-provider-from-spying-on-you/521208/ [https://perma.cc/93CK-TYS2].

90 Chris Ciaccia, *How Will ISPs Collect and Sell Your Browser History*, FOX NEWS (Mar. 30, 2017), https://www.foxnews.com/tech/how-will-isps-collect-and-sell-your-browser-history [https://perma.cc/TVS9-UP9C].

91 *See id.*

92 *See generally* Michael E. Lackey & Oral D. Pottinger, *Stored Communications Act: Practical Considerations*, LEXIS PRAC. ADVISOR J. (June 22, 2018), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/06/22/stored-communications-act-practical-considerations.aspx [https://perma.cc/7L48-JX8F].

93 *See infra* Part I.C.1; *see* Lackey & Pottinger, *supra* note 92.

94 18 U.S.C. §§ 2703–06 (2012).

electronic storage by that service."[95] Despite its modest protections, the SCA allows the government to compel an ECSP to disclose "a record or other information pertaining to a . . . customer" by court order.[96] Such an order (a "§ 2703(d) Order") allows law enforcement to circumvent the warrant requirement and access user data without facing traditional constitutional hurdles.[97] Moreover, the SCA does not provide a suppression remedy.[98] Thus, even if law enforcement garners evidence in violation of the SCA, the information at issue will still see its day in court.[99] The ease with which law enforcement can obtain a § 2703(d) Order illuminates a "loophole" around constitutional safeguards that the government capitalizes on when a target's data is stored by a third-party.[100]

---

[95] 18 U.S.C. § 2702(a)(1) (2012). The SCA carves out several exceptions to this general rule—one of which, created by the 2008 PROTECT Our Children Act, allows disclosure "to the [NCMEC], in connection with a report submitted thereto under [§] 2258A." 18 U.S.C. § 2702(b)(6).

[96] 18 U.S.C. § 2703(c)–(d). Under the SCA, only a non-content communication can be obtained via a § 2703(d) order. Since *Carpenter* does not acknowledge the "content/non-content" distinction emphasized by the SCA, discussed *infra*, this Note does not dive deeply into the distinction. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (reasoning that if email content received Fourth Amendment protection, the constitutional safeguard should also apply to CSLI data (meta-data)). The *Carpenter* Court also compared the privacy interest in CSLI, non-content data, to a privacy interest in physical letters held by a mail carrier and emails held by an ISP. *Id.* at 2230 (citing *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (letters held by mail carrier); United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010) (e-mails held by Internet service provider)).

[97] *See* 18 U.S.C. § 2703(d).

[98] *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820 (2003).

[99] *Id.*

[100] Orin S. Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, LAWFARE (June 26, 2018, 6:44 PM), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas [https://perma.cc/7CAY-XGXQ]. Criminal procedure allows for two types of compulsory process: a warrant or a subpoena. The first path, a warrant, allows officers to physically enter a particularly described location and take any evidence they find, subject to the warrant's terms. Search warrants are regulated by the Fourth Amendment, which provides several constitutional safeguards on what can be searched; the most notable being the probable cause and reasonableness requirements. Alternatively, law enforcement can gather evidence through an administrative

Further, ECSPs, unlike government actors, are not subject to constitutional constraints.[101] Therefore, when evidence of criminal activity is obtained by an ECSP and turned over to law enforcement, the methods used to obtain that evidence are not subject to Fourth Amendment scrutiny.[102] Additionally, if a government search is preceded by a private search, such as one by an ECSP, the search will not trigger constitutional protections.[103]

The unique ability of a private entity to access sensitive consumer information, combined with the dynamic between law enforcement and ECSPs, has hindered the Fourth Amendment's ability to protect privately held user information. This Note proposes a new Fourth Amendment framework for circumstances where law enforcement uses novel technologies to capitalize on private electronic information. The following Section discusses the Fourth Amendment and current framework for protecting such information.

B. The Fourth Amendment's Role in Protecting Information Privacy

The Fourth Amendment is our constitutional guarantee to be free from arbitrary government intrusion.[104] But, in the context of hashing, an ECSP's role as an intermediary between an individual and law enforcement renders most hash-evidence turned over to the government presumptively lawful under the private search

---

subpoena—which has similar requirements to a § 2703(d) Order. Unlike a warrant, a subpoena recipient is tasked with personally gathering the requested evidence. Since compliance with a subpoena implies certain statements—that the requested records exist, you possess the records, and you believe they are authentic—a recipient can claim his Fifth Amendment privilege against self-incrimination in response to the subpoena. Although the Fourth Amendment applies to a subpoena recipient, the protection is modest, and only allows the recipient to challenge the subpoena for being overbroad or unduly burdensome.

[101] United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *2 (E.D. Ky. June 23, 2017) ("[T]he Fourth Amendment protects individuals from 'unreasonable searches and seizures' by the government, not private entities.").

[102] *Id.* "The Fourth Amendment 'is wholly inapplicable' to searches and seizures by 'a private individual not acting as an agent of the Government.'" *Id.*

[103] *See infra* Part I.C.2.

[104] *See* U.S. CONST. amend. IV.

doctrine.[105] Additionally, courts have held that surveillance techniques that reveal information in the binary (such as hashing) do not infringe an objective expectation of privacy when law enforcement detects contraband.[106] Subsequently, all but one court addressing the Fourth Amendment implications of hash-evidence held that law enforcement's warrantless use of the evidence, obtained from an ECSP, was constitutional.[107]

However, the Supreme Court's 2018 decision in *Carpenter v. United States* fundamentally altered the constitutional framework for assessing the fit of novel technologies within preexisting Fourth Amendment doctrine.[108] In doing so, the Court cast doubt on the propriety of the third-party doctrine; which has reverberating effects on how the Fourth Amendment will be applied in the digital age.[109]

Although *Carpenter* marks a shift away from established Fourth Amendment principles, it is not the first time the Court has reevaluated how the amendment should be applied.[110] Moreover, the Fourth Amendment is dynamic and subject to periodic reevaluation as technology advances.[111] The following Subsection provides background on the Supreme Court's struggle to consistently apply the Fourth Amendment through shifting constitutional jurisprudence and technological advances.

---

[105] *Cf.* United States v. Jacobsen, 466 U.S. 109 (1984).

[106] Hash searches, like dog sniffs, provide information in binary: Either *yes*, the hash value of some file on a suspect's computer matches the hash value of some known piece of child pornography, or *no*, it does not. *See* Illinois v. Caballes, 543 U.S. 405, 408–09 (2005); United States v. Place, 462 U.S. 696, 707 (1983); *infra* Part I.C.4.

[107] *See, e.g.,* United States v. Ackerman, 831 F.3d 1292, 1306–08 (10th Cir. 2016); United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *8 (E.D. Ky. June 23, 2017); United States v. Reddick, 900 F.3d 636 (5th Cir. 2018). *But see* United States v. Crist, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008).

[108] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[109] *Id.*

[110] *See, e.g.*, United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001); Katz v. United States, 389 U.S. 347 (1967).

[111] *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

1. Reasonable Expectation of Privacy Test

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.[112] The Supreme Court has recognized that the "basic purpose" of the Fourth amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[113] However, for much of Fourth Amendment history, whether a government surveillance technique was deemed a "search," subject to constitutional scrutiny, was tied to common law trespass and focused on whether the government "obtain[ed] information by physically intruding [] a constitutionally protected area."[114]

Then, in response to law enforcement's rampant use of wiretaps, the Court reshaped Fourth Amendment protections by stating that the Fourth Amendment applies "to people, not places," and therefore is triggered when the government accesses information that an individual reasonably expects to remain private.[115] Justice Harlan's concurrence in *Katz* set forth a two-step test for determining whether an individual possesses a reasonable expectation of privacy ("REP") in what is searched or seized.[116] First, an individual must have an actual, subjective expectation of privacy ("subjective prong").[117] Second, one's subjective expectation must be recognized by society as reasonable ("objective prong.")[118] Existing customs, social policies, and norms determine which privacy expectations are objectively reasonable.[119]

Since *Katz*, the Supreme Court has grounded its Fourth Amendment decisions in whether an individual possessed a

---

112 U.S. CONST. amend. IV.
113 Camara v. Municipal Court of San Francisco, 387 U.S. 523, 528 (1967).
114 *Jones*, 565 U.S. at 406 n.3.
115 *Katz*, 389 U.S. at 351.
116 *Id.* at 361–63 (Harlan, J., concurring).
117 *Id.* at 361.
118 *Id*.
119 United States v. White, 401 U.S. 745, 787 (1981) (Harlan, J., dissenting) (privacy expectations reflect the customs and values of the existing society).

REP.[120] However, courts and scholars[121] alike have criticized a privacy-centric approach to Fourth Amendment protection in an era of significantly diminished privacy.[122] Moreover, the Supreme Court's ruling in *Carpenter* cast considerable doubt on the REP framework, which in turn has weakened the foundation on which doctrines grounded in a REP stand.[123]

The following sub-section begins by discussing the flaws of a privacy-centric approach to Fourth Amendment protection in an era where private corporations comprehensively track and share consumer behavior data.[124] Next, it analyzes the *Carpenter* Court's decision to deviate from a route application of the REP test, and focus on the class of information sought instead of the actions of law enforcement.[125] Third, it analyzes the third-party doctrine, which the *Carpenter* Court ruled does not extend to CSLI collected for more than seven days. Fourth, it examines the private search doctrine, a sub-set of the third-party doctrine. Finally, it considers the binary search doctrine. The following discussion of Fourth Amendment doctrine highlights *Carpenter*'s powerful impact on Fourth Amendment jurisprudence, far beyond the narrow fact-pattern before the Court.

---

[120] *See e.g.*, United States v. Kyllo, 533 U.S. 27 (2001); United States v. Knotts, 460 U.S. 276 (1983).

[121] Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 134 S. Ct. 2473 (2014); *see generally* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012).

[122] *See generally* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012).

[123] *See generally Carpenter*, 138 S. Ct. 2206.

[124] *See* Ohm, *supra* note 122, at 1310 ("Every year, companies, especially those that deliver services online, spend millions of dollars developing new services that track, store, and share the words, movements, and even the thoughts of their customers. These invasive services have proved to be irresistible to consumers, who have voluntarily embraced them in droves launching a social age of self-revelation.").

[125] *See generally Carpenter*, 138 S. Ct. 2206.

2. An Objective, Privacy-Centric Approach in a "World Without Privacy"

Courts have struggled to consistently apply both the subjective and objective prongs of the REP test since its inception.[126] Moreover, scholars have argued that the subjective component of the test has become a "phantom doctrine"[127]—reducing *Katz* to a "one step" inquiry: does society think it is reasonable to expect that the information or item sought by the government will remain private?[128]

The subjective prong of the REP test has lost its bite, because courts treat it as an inquiry into whether the citizen, in her mind, believed the information would remain private.[129] For example, did an individual *actually* believe that the content of her text messages, sent with a government-issued pager, would remain private?[130] The problem with this inquiry is that it never seems to matter.[131] A criminal defendant will (and should) always argue that they expected their information would be kept private from law enforcement's prying eye. Moreover, it is difficult to adduce evidence rebutting a person's self-reported mental state.[132] Thus,

---

[126] *See* Tom McInnis, *The Changing Definition of Search or Seizure*, 11 INSIGHTS ON L. & SOC'Y 10, 10–13 (2011) https://www.americanbar.org /content/dam/aba/images /public_education/presentations/ChangingDefinitionsofSearch.pdf [https://perma.cc/J3LJ-ME84]. Although part of the *Katz* test is supposed to be objective, without a standardized method for determining what personal expectations of privacy society is willing to accept, the conclusion has been depending on the shifting social and political views of the members of the Court. *Id.* at 12. *Compare* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imaging device to monitor radiation of heat from a person's home requires a warrant), *with* California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that aerial surveillance of a home does not violate the Fourth Amendment).

[127] Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015).

[128] *See generally id*.

[129] *Id.*

[130] *See* City of Ontario v. Quon, 560 U.S. 746 (2010).

[131] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. (forthcoming 2019) (manuscript at 57).

[132] This is not to say that a court will never find that a defendant lacked a subjective expectation of privacy. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that it is doubtful "people in general entertain any actual

the Court is almost never confronted with a scenario where the subjective prong of the REP test fails, but the objective prong does not.[133]

The *Carpenter* Court implicitly accepted the one-step approach to *Katz* by ignoring the test's subjective prong.[134] The opinion never mentioned the word "subjective," nor did it attempt to divide its analysis of the defendant's subjective and objective expectations of privacy.[135] But, as Professor Ohm states "*Carpenter* did not put a nail in the coffin of the subjective prong, because it was interred six feet under long ago."[136]

Further, premising Fourth Amendment protection solely on an objective, societally recognized privacy expectation is concerning in the digital era. Due to the vast amount of information Americans share with third-parties as a pre-requisite to be productive members of modern society,[137] and the growth of the "internet of things,"[138] it can be argued that there are few categories of

---

expectation of privacy in the numbers they dial"). Similarly, the prosecution very well may adduce sufficient evidence rebutting a defendant's claim that they actually expected their information to be kept private. *See, e.g.*, *id.* ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies 'for the purposes of checking billing operations, detecting fraud and preventing violations of law.'" (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977)).

133 *See* Ohm, *supra* note 131, at 56.

134 *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

135 Ohm, *supra* note 131, at 57.

136 *Id.* at 58; *see also* Kerr, *supra* note 127, at 114 (explaining that the subjective prong of the REP test was abandoned in the 1970s and 1980s).

137 *See generally Carpenter*, 138 S. Ct. 2206 (holding that using a cellphone is not "voluntary"); Riley v. California, 134 S. Ct. 2473 (2014) (emphasizing how a cell phone is vital to participation in modern life.).

138 The Internet of Things ("IoT") is the concept that almost any device with an on and off switch can be connected to the internet and other devices. The IoT thus makes up a network of connected devices and people. The analyst firm Gartner estimates that by 2020 there will be over 26 billion devices connected to the IoT. Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites

information that society reasonably believes will remain private.[139] To elaborate, the rise of cloud computing, social networking, and market reliance on Big Data, begets a world where citizens cannot reasonably expect that the majority of their digital data will remain private.[140]

As Professor Ohm warns, we are headed toward a "world without privacy."[141] In such a world, it would be futile for individuals to expect that most of their personal information will remain private. Thus, a Fourth Amendment built around reasonable expectations of privacy will no longer be effective.

C. Impact of United States v. Carpenter on the REP Test

As mentioned above the, the *Carpenter* Court did not engage in a two-step REP inquiry.[142] Instead, the Chief Justice enumerated three factors, aimed at the *class* of information sought, to

---

/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#2a401ae71d09 [https://perma.cc/LDY6-QFV7].

[139] *See id.* Since consumers know that many household products from refrigerators to toasters are now internet compatible, and often equipped with voice or video monitoring capabilities, people have a lesser expectation of privacy than in generations past.

[140] *See* Ohm, *supra* note 122, at 1317–18. First, cloud computing, the movement of computing and storage facilities to distant servers operated by ECSPs, led to billions of users storing their communications and writings with third-parties. Before the advent of could-based email services, like Gmail and Hotmail, people used email accounts provided by their employers or ISPs. Information on these accounts was saved periodically and locally. Now, billions of users systematically store messages and writings on third-party servers. Moreover, as discussed *supra*, user's metadata can be accessed by law enforcement with a mere court order—without a warrant or showing of probable cause. Next, the rise of social networking platforms capitalize on people's innate desire to connect with others. Since people feel connection (and entertainment) from using, and sharing personal information on these sites, the rise of social networking provides electronic service providers with mass amounts of user data that other types of ECSPs would never have access to. Finally, the widespread use of data analytics to monetize user data by drawing inferences, known as "Big Data," diminishes any expectation of privacy users have over their personal information. For example, companies can "re-identify" anonymized data by applying an algorithm. Even if users take measures to ensure that their data is anonymized, by removing any identifying markers, companies can restore the identity of the data's owner by analyzing patterns in the data. *Id.* at 1315–17.

[141] *See generally id*.

[142] *See generally Carpenter*, 138 S. Ct. 2206.

determine if the Fourth Amendment was invoked—marking a notable shift away from a Fourth Amendment analysis focused solely on privacy expectations.[143] Notwithstanding well-settled precedent that an individual lacks an objective expectation of privacy in business records maintained by a third party, the Court held that a search occurred when warrantless cell-site location information ("CSLI") records were obtained by the government.[144]

The *Carpenter* Court resolved whether a warrant is required for law enforcement to retrieve historic[145] CSLI, that is collected and maintained by private companies for legitimate business purposes.[146] A cell-site is a cellular telephone "tower," owned by a wireless carrier, where radio signals are received from customer's cell phones.[147] When a cell phone user makes a call, sends a text message or email, accesses the internet, or in any way connects to their cellular network, their cell-phone establishes a radio connection with the closest cell-tower.[148] Wireless service providers create records ("CSLI records") each time a cell-phone connects to a specific tower.[149] As a cell phone user moves, their

---

[143] *Id.* at 2223.

[144] *Id.* Probable cause is only required if CSLI records are collected for more than six days. *Id.* at 2224 (Kennedy, J., dissenting).

[145] Historical location information refers to "[r]ecords stored by the wireless service provider that detail the location of a cell phone in the past (i.e.: prior to entry of the court order authorizing government acquisition)." Prospective location information refers to "all cell site information that is generated after the government has received court permission to acquire it." You may also come across the term "real time" location information. This is a subset of prospective location information, and "refers to data used by the government to identify the location of a phone at the present moment." *In re* Application for Order of a Pen Register, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

[146] *See generally Carpenter*, 138 S. Ct. 2206.

[147] *Cell Phone Location Tracking*, BERKELEY L., https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/3YVE-R6NX] (last visited Jan. 30, 2019).

[148] *Carpenter*, 138 S. Ct. at 2225 (Kennedy, J., dissenting).

[149] *Id.* Compare the information revealed in CSLI records at issue in *Carpenter* (for a phone call, a wireless service provider records the date, time, and duration of the call; the phone numbers making and receiving the call; the cell site "pinged" when the call was made, and the specific connection that made the connection, in its CSLI record) with the pen register used in *Smith v. Maryland*. *See* 422 U.S. 735, 742 (1979).

phone will send radio signals to multiple cell towers.[150] The location of these cell towers can be used to estimate the location of an individual through triangulation.[151]

The circumstances giving rise to the *Carpenter* case arose after police arrested four men suspected of a string of robberies of, ironically, T-Mobile stores.[152] One of the men confessed, and provided police with the phone numbers of several accomplices.[153] Based on this information, prosecutors applied for a § 2703(d) Order to obtain cell-phone records for Carpenter and several others.[154] Two orders were granted directing Carpenter's wireless carrier, Sprint, to produce his cell-site location information ("CSLI") to law enforcement.[155] Between the two orders, the government obtained 12,898 location points cataloging the defendant's movements over 127 days.[156] At trial, the prosecution offered the CSLI records to show that the defendant was near four of the robbery locations at the time they occurred.[157] The defendant's motion to suppress the CSLI evidence was denied, and he was convicted.[158] The Sixth Circuit affirmed the lower court's holdings.[159] Ultimately, the Supreme Court held that law enforcement may not collect historical CSLI for more than seven days without a warrant.[160] More importantly, it held that CSLI is

---

150 *See* BERKELEY L., *supra* note 147.
151 *Id.*
152 *Carpenter*, 138 S. Ct. at 2212.
153 *Id.*
154 Pursuant to the SCA, law enforcement can require a wireless carrier to disclose "a record or other information pertaining to a subscriber to or customer of such service . . . when the government entity . . . offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. §§ 2703(c)–(d) (2010); *supra* Part I.A.3. Although what constitutes "probable cause" is debated and fact specific, the reasonable suspicion standard is significantly lower than the probable cause standard. *See* Illinois v. Gates, 462 U.S. 213, 235 (1983).
155 *Carpenter*, 138 S. Ct. at 2212.
156 *Id.*
157 *Id.* at 2212–13.
158 *Id.*
159 *Id.* at 2213.
160 *Id.* at 2217 n.3.

protected "[w]hether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier."[161]

When assessing whether information was "searched," the *Carpenter* court shifted away from the *Katz* REP analysis, to a multi-factor test.[162] Justice Roberts set forth three factors, aimed at the category of information sought by law enforcement.[163] Lower courts assessing whether a search of information held by a third-party occurred must now ask whether the category of information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection.[164]

Notably, the Court's focus on the type of information sought, alone, marks a fundamental shift in Fourth Amendment jurisprudence, which traditionally focuses on the actions taken by law enforcement while obtaining such information.[165] Under Robert's new test, a court determining whether a search occurred will assess the "depth" and "breadth" of information held by a third-party.[166] Since there are no mandatory data retention regulations governing ECSPs, it is up to the individual company to decide how long to retain consumer data.[167] Therefore, when applied, the "depth" and "breadth" factor discussed by Roberts will mandate that a district court delve into the decisions of private businesses, specifically: how long the business keeps consumer

---

161 *Id.* at 2217.
162 *See id.* at 2223.
163 *Id.*
164 *Id.*
165 *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (asserting that the "reasonableness" requirement of the Fourth Amendment has been consistently construed to regulate governmental action); Katz v. United States, 389 U.S. 347, 353 (1967) (scrutinizing law enforcement's actions to determine whether the Fourth Amendment was violated).
166 *Carpenter*, 138 S. Ct. at 2223.
167 *See* Ernesto Van der Sar, *How Long Does Your ISP Store IP-Address Logs?*, TORRENT FREAK (June 29, 2012), https://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629/ [https://perma.cc/KSJ5-26VL].

data and how much data it keeps, in assessing whether a search occurred.[168]

The next Subsection will discuss *Carpenter*'s determination that CSLI is protected even when the government leverages the technology of a wireless carrier, which is a marked departure from the third-party doctrine. The third-party doctrine is grounded in the REP approach.[169]

1. The Third-Party Doctrine

The third-party doctrine, as articulated in *Smith* and *Miller*, states that an individual does not retain a reasonable expectation of privacy in non-content information voluntarily conveyed to third parties, such as telephone numbers or bank records.[170] Thus, such information does not receive Fourth Amendment protection. [171] The rationale underlying the third-party doctrine stems from two common law rules: the "assumption of risk"[172] doctrine and the "voluntary exposure"[173] doctrine.

First, the Supreme Court has held that when a person shares secrets with another, they "assume the risk" of disclosure and lose any Fourth Amendment protection over that information, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third-

---

[168] *See Carpenter*, 138 S. Ct. at 2223. Companies must balance the potential benefits of having access to old data, against the cost of storing data, and threats of a breach, in formulating their data retention policies. *See* Ohm, *supra* note 131, at 31–32.

[169] The *Smith* Court held, after "applying the *Katz* analysis," that the defendant did not possess a REP in metadata collected by a pen register since "people in general [do not] entertain any actual expectation of privacy in the numbers they dial." 442 U.S. 735, 741–42 (1979) (holding "all telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").

[170] United States v. Miller, 425 U.S. 435, 442 (1976); *Smith*, 442 U.S. at 743–44.

[171] *Smith*, 442 U.S. at 745–46.

[172] Hoffa v. United States, 385 U.S. 293, 303 (1966).

[173] Katz v. United States, 389 U.S. 347, 351 (1967); *see also* Dow Chem. Co. v. United States, 476 U.S. 227, 230 (1986) (articulating the "knowing exposure" doctrine).

party will not be betrayed."[174] Second, the Court held in *Katz* that "[w]hat a person *knowingly* exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[175]

Based on the assumption of risk and voluntary exposure rules, the *Miller* Court, applying the *Katz* test, reasoned that a person cannot subjectively expect that what he knowing tells a third-party will, in every case, remain secret.[176] *Miller* also emphasized that no objective privacy expectation exists to protect against the risk that information related to another may be eventually given to the government.[177] This proposition has come to be known as the third-party doctrine.[178] Courts have categorically applied the third-party doctrine to circumstances where information shared online with an ECSP is later accessed by the police.[179]

Although *Carpenter*'s precise impact on the third-party doctrine is hotly debated, the Court rejected the longstanding view that the doctrine categorically prohibited a Fourth Amendment analysis whenever information is voluntarily conveyed to a third-

---

[174] *Miller*, 425 U.S. at 443. *See also* United States v. White, 401 U.S. 745 (1971) (deciding electronic surveillance of voluntary conversations between defendant and an informant does not constitute Fourth Amendment violation); *Hoffa*, 385 U.S. at 293 (1966) (finding that defendant's trust in an accomplice does not create a legitimate expectation of privacy which would be infringed by the accomplice's delivery of incriminating information to the government).

[175] *Katz*, 389 U.S. at 351 (emphasis added).

[176] *Miller*, 425 U.S. at 449.

[177] *Id.* at 443 ("The depositor takes the risk that the financial information he reveals to the bank may be relayed to the government.").

[178] *See id.* at 435; Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[179] *See* United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (holding that individuals have no reasonable expectation of privacy in CSLI); ACLU v. Clapper, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013) (finding that the National Security Agency's mass metadata collection program did not violate the Fourth Amendment because of the third-party doctrine); United States v. Graham, 846 F. Supp. 2d 384, 400 (D. Md. 2012) (holding that historical CSLI is not protected by the Fourth Amendment because of the third-party doctrine); *see also* Ohm, *supra* note 122, at 1327–28 ("A court could reasonably hold that some of the content posted to Facebook has been knowingly exposed to the public, and following conventional Fourth Amendment law, rule that it may be obtained by the police without a warrant.").

party.[180] After rejecting a bright-line rule, the Court implicitly adopted petitioner's argument that the third-party doctrine only "diminishes the degree of privacy;" and set up a hierarchical standard that focuses on the nature of the *information* sought; to determine the proper, subsequent Fourth Amendment analysis.[181] Put differently, individuals will retain a diminished privacy interest in information that is more revealing, comprehensive, and inescapably collected, than the information at issue in *Smith* and *Miller*.[182] Additionally, a third-party's maintenance of such information will not render it automatically outside of the Fourth Amendment's scope.[183]

Before assessing the private search doctrine, it is helpful to discuss its intimate connection to the third-party doctrine.[184] After all, the private search doctrine stems from the same rationales and implicates the same issues with ECSPs as the third-party doctrine.[185] Both the private search and third-party doctrines rely on the idea that "[a] private search extinguishes an individual's reasonable expectation of privacy in the object searched . . . ."[186] In both circumstances, courts have held that once frustration of an individual's expectation of privacy occurs by a private actor, the

---

[180] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) ("[T]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information collected by wireless carriers."); *cf.* Riley v. California, 134 S. Ct. 2473, 2478 (2014) (rejecting the formerly categorical application of the search incident to arrest doctrine articulated in Robinson and holding that a cell-phone cannot be searched incident to a lawful arrest).

[181] Brief for Petitioner at 10, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

[182] *Carpenter*, 138 S. Ct. at 2223.

[183] *See id.* at 2217, 2223; Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/F5AU-JZUB].

[184] *See Carpenter*, 138 S. Ct. at 2217.

[185] *See id.*

[186] Priscilla Grantham Adams, *Fourth Amendment Applicability: Private Searches*, U. MISS. SCH. L.: NAT'L CTR. FOR JUST. & RULE L. 1–2 (2008), http://www.olemiss.edu/depts/ncjrl/pdf/PrivateSearchDoctrine.pdf [https://perma.cc/BG38-TE6E].

Fourth Amendments does not prohibit governmental use of the now "non-private information."[187]

Justice White, in his concurrence in *Jacobsen*, notes that the private search doctrine "shares many of the doctrinal underpinnings of cases establishing that 'the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.'"[188] Moreover, in first articulating the private search doctrine as we conceptualize it today, Justice Stevens explained that the rule "follows from the analysis applicable when private parties reveal other kinds of private information to the authorities."[189] He supports this assertion by noting that the Court repeatedly held that the Fourth Amendment does not prohibit Government use of information revealed by a third-party, even if that information was revealed "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[190] Justice Stevens' quote comes directly from *Miller,* the case articulating the third-party doctrine.[191]

2. Private Search Doctrine

The Court addressed the implications of a private party revealing information to law enforcement, outside of the context of records held by a third-party, in *United States v. Jacobsen*.[192] In *Jacobsen*, two FedEx employees opened a damaged package pursuant to a company policy regarding insurance claims.[193] Upon inspecting the package, the employees found a series of four zip lock bags, the innermost containing six and a half ounces of white powder.[194] The employees notified law enforcement ("DEA"), and placed the plastic bags back inside the package.[195] When the DEA

---

187 United States v. Jacobsen, 466 U.S. 109, 117 (1984).
188 *Id.* at 130 (White, J., concurring) (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).
189 *Id.* at 117 (majority opinion).
190 *Id.* (quoting *Miller*, 425 U.S. at 443).
191 *See id.*
192 *See generally id.*
193 *Id.* at 111.
194 *Id.*
195 *Id.*

agent arrived, he opened the package from the end that had already been visibly opened by the employees, opened each bag, and removed a small amount of white substance to submit to a field test for cocaine.[196] Jacobsen challenged the DEA's opening of the package and testing of the powder as a warrantless search in violation of his Fourth Amendment rights.[197] Expanding on its recent decision in *Walter*, [198] the majority concluded that the DEA agent had not conducted a "search," because he had not exceeded the scope of the previous private search when he opened the package and removed the plastic bags.[199] In explaining its rationale, the Court explicitly based its conclusion on the assumption of risk doctrine: when a party reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs, the Fourth Amendment does not prohibit governmental use of that information.[200] Moreover, the Court restated its holding in *Miller*, that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and then conveyed by him to Government authorities."[201]

Today, *Jacobsen* stands for the proposition that a government search that merely replicates a previous private search is not subject to Fourth Amendment scrutiny.[202] A constitutional analysis

---

196 *Id.* at 111–12.

197 *See infra* Part I.C.4 (discussing the role of the binary search doctrine in *Jacobsen*.).

198 The Supreme Court in *Walter* held that law enforcement's warrantless viewing of contraband video, voluntarily given to them a private party, who viewed portions of the video, constituted a Fourth Amendment search. Since law enforcement gained substantially more knowledge from viewing the video than it had when it received the video from the private party, its actions expanded the formerly private search and required probable cause. Walter v. United States, 447 U.S. 649 (1980).

199 *Jacobsen*, 466 U.S. at 116–20.

200 *Id.* at 117 ("This standard follows from the analysis applicable when private parties reveal other kinds of private information to the authorities. It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.").

201 *Id.* at 117 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

202 *See generally id.*

is only triggered if the government search exceeds the scope of the private search.[203] Further, since the Constitution proscribes only government action, the Court has held that regardless of whether private action is reasonable or unreasonable, accidental or deliberate, it does not violate the Fourth Amendment because of its private nature.[204]

3. The Private Search Doctrine in Hashing Cases

All but one federal court[205] ruled that law enforcement's acquisition and use of hash-evidence is not a Fourth Amendment search, because an ECSP typically identifies the "matching" images as contraband and submits them to NCMEC before law enforcement views them: implicating the private search doctrine.[206]

---

[203] *See Walter*, 447 U.S. at 657.

[204] *Jacobsen*, 466 U.S. at 115.

[205] In 2008, the Middle District of Pennsylvania was the first court to address the Fourth Amendment implications of warrantless hash-value matching in *United States v. Crist*. Although the Crist court concluded that the "running of hash values" is a search protected by the Fourth Amendment, the case is inapplicable to this Note for two reasons. First, the private search that uncovered child pornography on Crist's computer was conducted by a human—not an ECSP. Second, the Court swiftly held, without rationale, that by "subjecting [an] entire computer to a hash value analysis –every file, internet history, picture, and 'buddy list' became available for government review [and] [s]uch examination constitutes a search." This proposition is inaccurate because it misconstrues what hashing exposes to an observer. First, hash-values are predictors of data that reveal no more about content than a random number. Thus, exposing a hash-value to a government agent does not allow the agent to "review" the underlying file, in the sense the *Crist* court indicated. *See* 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008). The Court in *United States v. Keith* expressed this proposition by holding that "matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file." Second, unlike a label, a hash-value has no inherent meaning. *See* 980 F. Supp. 2d 33, 43 (D. Mass. 2013). The *Miller* Court, in regard to Google's hashing policy, explained that a hash value only acquires meaning "when it matches with a hash value in the child pornography repository and therefore reminds Google that it has seen this image before." United States v. Miller, 2017 WL 2705963, at *5 (E.D. Ky. June 23, 2017). Lastly, the hashing process only works in one direction and a government agent cannot "reverse" a hash-value back to the file it identified. *See supra* Part I.A.

[206] *See infra* Part I.A.3.

Last year, the Fifth Circuit mechanically applied the private search doctrine in denying a motion to suppress hash-evidence in *United States v. Reddick*.[207] In *Reddick*, a Microsoft user uploaded a digital file to Microsoft Skydrive, a cloud hosting service.[208] Skydrive employs a program called PhotoDNA, which discerns the hash values of user uploaded files and compares them against the hash values of known child pornography.[209] Based on a hash value match between defendant's file, and a file known to contain child pornography, Microsoft sent the file and defendant's Internet Protocol ("IP") address to NCMEC's CyberTipline.[210] NCMEC then sent its report ("CyberTip") to the local police department where the defendant lived.[211] Upon receiving the CyperTip, a detective opened each of the suspect files, confirmed they contained child pornography, and applied for a warrant to search defendant's home.[212] Defendant was arrested, and following his indictment, he moved to suppress all evidence of child pornography on the grounds that the detective's warrantless opening of the files associated with the CyperTip was an unlawful search.[213] The District Court denied defendant's motion, holding that although the detective's viewing of the files invaded a constitutional expectation of privacy, the evidence supported a good faith exception to the exclusionary rule.[214] The Fifth Circuit affirmed, but disagreed with the district court that the initial viewing of the files violated the Fourth Amendment.[215] The Circuit Court reasoned that the present situation fell squarely within the private search issue presented in *Jacobsen*—analogizing the

---

[207] *See generally* United States v. Reddick, 900 F.3d 636 (5th Cir. 2018).

[208] "Cloud server hosting is when hosting services are made available to customers on demand via the Internet. Rather than being provided by a single server or virtual server, cloud server hosting services are provided by multiple connected servers that comprise a cloud." Vangie Beal, *Cloud Server Hosting*, WEBOPEDIA https://www.webopedia.com/TERM/C/cloud_server_hosting.html [https://perma.cc/Z76R-6827] (last visited Jan. 31, 2019).

[209] *Reddick*, 900 F.3d at 637–38.

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] *Id.*

[214] *Id.*

[215] *See supra* Part I.C.2 (discussing the private search doctrine).

contents of the files defendant uploaded to a physical package. [216] The Court reasoned that when the defendant uploaded the files to SkyDrive, Microsoft's PhotoDNA program automatically reviewed them and compared them against an existing database.[217] Accordingly, Microsoft, a private actor "inspected and deemed [defendant's 'package'] suspicious," before its contents were turned over to law enforcement, thereby frustrating any expectation of privacy the Defendant had in his files.[218]

The analysis employed by the *Reddick* Court is consistent with other courts addressing the private search issue arising from the acquisition of hash-evidence.[219] Since the private search doctrine was so firmly rooted in Fourth Amendment jurisprudence before *Carpenter*, courts faced with motions to suppress hash-evidence only analyzed whether: (1) law enforcement's activities exceeded the scope of the ECSP's private search; and (2) whether ECSP's are government "agents" for purposes of the Fourth Amendment.[220]

The first issue, regarding the scope of the private search, requires a fact-specific inquiry into the actions of law enforcement upon receiving a NCMEC report. However, absent clear government overreach, all courts have found that a detective's visual review of suspect images attached to a NCMEC report did

---

[216] "The exact issues presented by this case may be novel. But the governing constitutional principles set forth by the Supreme Court are not. The government effectively learned nothing from Detective Ilse's viewing of the files that it had not already learned from the private search. Accordingly, under the private search doctrine, the government did not violate Reddick's Fourth Amendment rights." *Reddick*, 900 F.3d at 640.

[217] *Id.* at 639.

[218] *Id.*; *see also* United States v. Jacobsen, 466 U.S. 109 (1984).

[219] *See, e.g.*, United States v. Ackerman, 831 F.3d 1292 (2016); United States v. Miller, 2017 WL 2705963 (E.D. Ky. June 23, 2017).

[220] Since this Note argues that the Court deviate from the REP based private search doctrine, an analysis of the scope of a private search and government agency are outside the purview of the current discussion. *But see, e.g.*, *Ackerman*, 831 F.3d 1292 (holding that law enforcement exceeded the scope of AOL's private search, when a detective opened *four* images attached to a NCMEC report, and only *one* of the images had matched a hash-value of a confirmed child pornographic image); *Miller*, 2017 WL 2705963 (holding that Google is not a government agent when it voluntarily scans email attachments for apparent child pornography).

not exceed the scope of the initial private search, because the detective knew with virtual certainty what the files contained.[221] Further, no court has held that the PROTECT Act's reporting dynamic renders ECSP's government actors for Fourth Amendment purposes.[222]

4. The Binary Search Doctrine

Moreover, in addition to the barrier erected by the private search doctrine, a defendant typically cannot suppress hash-evidence because hash-value matching reveals information in the "binary."[223] Put differently, hash-value matching indicates the presence or absence of contraband, and nothing else.[224]

The constitutionality of a different type of binary search—a field test for cocaine—was first raised in *Jacobsen*.[225] There, the Court held that the test did not constitute a search pursuant to the binary search doctrine—articulated in dicta of *United States v. Place*.[226]

In *United States v. Place*, the Supreme Court addressed the Fourth Amendment's relevance to surveillance techniques that purportedly reveal only the presence or absence of contraband.[227] In *Place*, the Court addressed whether the Fourth Amendment bars

---

[221] *See Jacobsen*, 466 U.S. at 119 (employing "virtual certainty" test for determining scope of private search); *Reddick*, 900 F.3d at 639 (holding that the detective's visual review of the files attached to a NCMEC report did not "'significant[ly] expan[d] the search that had been conducted previously by a private party,' sufficient to constitute 'a separate search'"); *Miller*, 2017 WL 2705963, at *4 (holding that the detective did not exceed Google's private search since the detective had "near-certainty regarding what [he] would find and little chance to see much other than contraband").

[222] *See, e.g.*, United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) (holding that AOL was not a "mere conduit" for the government and was thus not a government agent); *Miller*, 2017 WL 2705963, at *2 (holding "Google is not a government actor"); *cf.* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (providing the rule that in the context of the Fourth Amendment, if a private individual conducts a search "as an instrument or agent of the Government," that search is subject to constitutional scrutiny).

[223] *See* United States v. Place, 462 U.S. 696, 707 (1983).

[224] *See supra* Part I.A.1.

[225] *Jacobsen*, 466 U.S. 109.

[226] *Id.* at 123–24 (citing *Place*, 462 U.S. at 707).

[227] *Place*, 462 U.S. at 707.

law enforcement from temporarily detaining personal luggage for exposure to a canine sniff on the basis of a reasonable suspicion.[228] The majority concluded that *Terry* allowed the agents to briefly detain the passenger's luggage.[229] In arriving at this conclusion, the Court noted that the passenger's luggage was seized to arrange its exposure to a narcotics detection dog.[230]

Thus, the Court addressed, in dicta,[231] whether the use of a narcotics detection dog was a "search."[232] If so, the Court reasoned, "the initial seizure of respondent's luggage for the purpose of subjecting it to the sniff test—no matter how brief—could not be justified on less than probable cause."[233] The majority answered this question in the negative, stating that "the canine sniff is *sui generis* . . . no other investigative procedure [] is so limited both in the manner in which the information is obtained and in the content of the information revealed."[234] Specifically, "[a] 'canine sniff' . . . does not expose noncontraband items that otherwise would remain hidden from public view," ensuring that "the owner of the property is not subjected to the embarrassment and inconvenience entailed in . . . more intrusive investigative methods."[235] Additionally, the Court reasoned, "the sniff discloses only the presence or absence of narcotics, which is a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information is limited."[236]

Although the Court's categorization of a canine sniff as "*sui generis*" was quickly contradicted, the reasoning articulated in *Place*—that a minimally intrusive technique which only reveals the

---

228 *Id.* at 699.
229 *Id.* at 706.
230 *Id*.
231 Lower courts "are bound by the Supreme Court's considered dicta almost as firmly as by the Court's outright holdings, particularly when . . . a dictum . . . [is] not enfeebled by any subsequent statement." McCoy v. Mass. Inst. of Tech., 950 F.2d 13, 19 (1st Cir. 1991).
232 *Place*, 426 U.S. at 706.
233 *Id*.; *see* Terry v. Ohio, 392 U.S. 1, 20 (1968).
234 *Place*, 426 U.S. at 707.
235 *Id.*
236 *Id.*

presence or absence of a contraband item—was applied the following year in *Jacobsen*.[237]

The *Jacobsen* Court considered whether a field test, used to determine if a "suspicious white powder was cocaine . . . [and] nothing more" violated an expectation of privacy that society considered reasonable.[238] Based on *Place*, the majority held that "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest."[239] The *Jacobsen* majority contrasted a societally recognized expectation of privacy, protected by the Fourth Amendment, with a mere subjective belief that information will be kept private.[240] The Court interestingly employed the example of "information voluntarily disclosed to a government[] informant" as information over which a defendant may have an actual expectation of privacy that is *not* objectively reasonable.[241] Emphasizing the importance of the REP test's objective prong, the Court held that the narcotics field test did not constitute a search.[242]

Subsequent cases addressing surveillance techniques that provide information in the binary have shifted away from the two-factor analysis employed by *Place* and *Jacobsen*, focusing solely on the binary nature of the technique, and ignoring the level of intrusiveness on the citizen.[243] Scholars have labeled this approach taken by courts as the "pure binary search doctrine."[244]

The policy implications of the binary search doctrine have faced considerable criticism, especially as surveillance technology

---

[237] The year after *Place* was decided, the Supreme Court analyzed another binary authentication method—a narcotics field test—under the Fourth Amendment in *United States v. Jacobsen*. 466 U.S. 109 (1984).

[238] *Jacobsen*, 466 U.S. at 122.

[239] *Id.* at 123.

[240] *Id*. at 122.

[241] *Id.* at 123.

[242] *Id.*

[243] *Compare* United States v. Place, 462 U.S. 696, 707 (1983), *and* Indianapolis v. Edmond, 531 U.S. 32, 40 (2000), *with* Illinois v. Caballes, 543 U.S. 405, 408 (2005).

[244] Laurent Sacharoff, *The Binary Search Doctrine*, 42 HOFSTRA L. REV. 1139, 1145 (2014).

becomes more precise.[245] The *Place* line of cases implies that the more tailored a surveillance technique is to detecting contraband, the less Fourth Amendment protection the public will have over what is being surveilled.[246] This logic directly contradicts an "equilibrium adjustment"[247] theory of the Fourth Amendment, and common sense. In criticizing the binary search doctrine, Aya Gruber[248] asserts that:

> [i]f *Caballes* stands for the broad proposition that there is no search when only contraband is detected, then the government is free to deploy such contraband detecting devices in each and every one of our house on the ground that if we are innocent, we have nothing to hide . . . all these devices could be employed on the sole bases of police hunches, whims, prejudices, or anything at all, because they are beyond the purview of the Fourth Amendment.[249]

Moreover, the binary search doctrine is inconsistent with Fourth Amendment formalism—the prevailing school of thought on Fourth Amendment theory.[250]

5. Formalist Approach to the Binary Search Doctrine

Analyzing the constitutionality of the binary search doctrine requires a brief discussion of competing approaches to Fourth Amendment rights: the formalist approach and the innocence

---

[245] *See* Jacobsen, 466 U.S. at 135–38 (Brennan, J., dissenting); Salgado, *supra* note 8.

[246] Marcia Hofmann, *Arguing for Suppression of 'Hash' Evidence*, CHAMPION, May 2009, at 20, 23.

[247] *See infra* Part I.A.

[248] Aya Gruber is a Professor of Law at the University of Colorado Law School and Scholar in the fields of gender and race law. *Aya Gruber*, COLO. L., https://lawweb.colorado.edu/profiles/profile.jsp?id=325 [https://perma.cc/5QFV-RZS3] (last visited Jan. 31, 2019).

[249] Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. DAVIS L. REV. 781, 823–24 (2008).

[250] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018); United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001).

approach.[251] This Subsection reviews the competing approaches, in favor of the formalist view.

Formalism, the majority approach, focuses solely on the quantum of evidence gathered by the state before conducting a search, and declines to identify or articulate any continuum of privacy entitlement turning on individual conduct.[252] Formalism views the key feature of the amendment as the duties it places on government actors.[253] Thus, an individual's behavior—their guilt or innocence—is irrelevant in analyzing the scope of their constitutional protection.[254] Under the formalist view, any violation of the Fourth Amendment constitutes cognizable harm, even if the subject of the search is factually guilty.[255]

Although formalism is the prevailing approach to the Fourth Amendment, the Supreme Court recognizes co-existing theories, allowing it to choose which theory to apply based on the specific facts of a given case.[256] The binary search cases represent an innocence model of Fourth Amendment theory,[257] which implies that harm only occurs when an innocent person is illegally searched.[258] Such a model confers a greater privacy entitlement to the innocent than the guilty.[259] The innocence model views the

---

[251] *See* Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1462–63 (1996).

[252] *Id.* at 1466–67.

[253] *Id.*

[254] *Id.* at 1467.

[255] *Id.* "The set of parties injured by unreasonable searches thus consists of all persons searched without the appropriate level of pre-search knowledge on the part of the relevant public official. Accordingly, when the public official has the requisite prior knowledge, there is no violation of the right of privacy and no constitutional harm." *Id.*

[256] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 507 (2007).

[257] United States v. Jacobsen, 466 U.S. 109, 123 (1984) ("It is probably safe to assume that virtually all of the tests conducted under circumstances comparable to those disclosed by this record would result in a positive finding; *in such cases, no legitimate interest has been compromised*." (emphasis added)).

[258] *See id.* at 137.

[259] *C.f. id.* (The binary search doctrine can only be supported by an innocence theory of Fourth Amendment jurisprudence that assumes that the Fourth Amendment protects only the innocent.) In articulating the doctrine, the *Jacobsen* Court held that "Congress has decided-and there is no question about

Fourth Amendment as an "imperfect divining rod," aimed at maximizing the number of "ideal" searches—those that reveal evidence of a crime.[260] Arnold Loewy, a proponent of the innocence model, describes a hypothetical "divining rod" to demonstrate the goal of the Fourth Amendment under the innocence model:

> In a Utopian society, each policeman would be equipped with an evidence-detecting divining rod. He would walk up and down the streets and whenever the divining rod detected evidence of crime, it would locate the evidence. First, it would single out the house, then it would point to the room, then the drawer, and finally the evidence itself. Thus, all evidence of crime would be uncovered in the most efficient possible manner, and no innocent person would be subject to a search. In a real society (such as ours), the fourth amendment serves as an imperfect divining rod.[261]

Loewy's divining rod, which he hypothesized in 1983, posits a perfectly efficient binary search.[262] In the context of child pornography prosecutions, Loewy's divining rod exists—hash-value matching.[263] The propriety of Loewy's approach boils down to which harms one believes the Fourth Amendment is intended to prevent. This Note agrees with the formalist view that society has a collective right to government compliance with the Fourth Amendment, therefore, a violation of the right constitutes harm even when it reveals evidence of criminal wrongdoing.

---

its power to do so-to treat the interest in 'privately' possessing cocaine as illegitimate; thus governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest." *Id.* at 123. Thus, the Court based its articulation of the doctrine on the proposition that there is no Forth Amendment protection over illicit activity; an innocence theory of the amendment.

260 *See generally* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983).

261 *Id.* at 1244.

262 *See id.*

263 *See supra* Part I.A.1.

The Court's endorsement of a formalist approach to the Fourth Amendment is illustrated by its focus on state action when reviewing a motion to suppress evidence.Whether a defendant can utilize his Fourth Amendment rights (and move to exclude evidence against him) depends on the actions of a third-party. Specifically, this inquiry focuses on whether the *state* has established probable cause.[264] The Court's focus on state action is further exemplified by judicially recognized exceptions, "excusing" officers from the probable cause requirement on the premise that their behavior was justified by, among other reasons, fear for their own, or public safety.[265] The result of this state-focused analysis is that an individual retains a privacy right until the state acquires enough knowledge of criminal activity to invade that right.[266]

The paradox of defining an individual right by the conduct of someone aside from the right holder can be rationalized by viewing an analog, collective right to the Fourth Amendment *procedure* itself, implicating different policy concerns than those implicated when one's substantive right is violated.[267] Thus, in an important sense, the right conferred by the amendment is that the government complies with its probable cause and reasonableness requirements.[268] If a collective right is recognized to safeguard procedure, all of society is harmed when that procedure is not complied with.[269]

A proponent of the innocence approach may counter the above assertion by correctly noting that the boundaries of a Fourth Amendment right holder's protection are partially determined by

---

264 *See* U.S. CONST. amend. IV; *see also* Loewy, *supra* note 260 at 1240.

265 *See, e.g.*, New York v. Quarles, 467 U.S. 649 (1984) (articulating the public safety exception to the warrant requirement); Terry v. Ohio, 392 U.S. 1, 3 (1968) (establishing that if a police officer has a reasonable suspicion that a suspect has committed, is committing, or is about to commit a crime and has a reasonable belief that the person "may be armed and presently dangerous," the officer can briefly seize and search the suspect without a warrant).

266 *See* U.S. CONST. amend. IV.

267 *See* U.S. CONST. amend. IV. The Fourth Amendment provides a substantive right to be free from unreasonable government scrutiny. *See id.*

268 *See id.*

269 *See id.*

their own actions. For example, an individual can forfeit their right in multiple ways, such as indicating the lack of an expectation of privacy or creating circumstances that are objectively dangerous to law enforcement or society.[270] However, if an analog collective right to procedural integrity is recognized, an unreasonable search that uncovers evidence of a crime is still unconstitutional.[271] In such a scenario, an individual may have forfeited her substantive right to be free of unreasonable government scrutiny, but, the state still violated society's collective right securing procedural indignity by invading a target's privacy without a sufficient evidentiary foundation.[272]

II. FOURTH AMENDMENT EXCEPTIONALISM

> *"The Constitution is premised on an ordinary rate of change in the balance of power between the state and the people. The Fourth Amendment is our national thermostat, recalibrating what the police can and cannot do."*[273]

In an era of unprecedented technological innovation, the Court must grapple with *when* and *how* to adjust the scope of the Fourth Amendment to maintain its core protections. Regarding the *when*, this Note argues that if a new technology is "exceptional," the law must inevitably adjust its approach to assessing disputes arising from that technology. An exceptional technology is one that disrupts the balance of power maintained by the Fourth Amendment.[274] Regarding the *how*, this Note proposes that Courts should decline to apply traditional, "mono-analogical"[275] reasoning

---

[270] *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 323 (1987) (establishing that leaving evidence in plain view forfeits privacy right); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that knowing exposure of information to a third-party forfeits one's Fourth Amendment protection).

[271] *See* U.S. CONST. amend. IV.

[272] *See id.*

[273] Ohm, *supra* note 131, at 59.

[274] *See infra* Part I.A.1.

[275] "The term 'mono-analogical' designates a brand of analogical reasoning where only a single dimension of a subject is mapped." Luke M. Milligan,

in assessing whether a novel technology is subject to a pre-existing legal doctrine.[276] Mono-analogical reasoning refers to a type of analogical reasoning where only a single dimension of a subject is mapped—typically, the subject's function.[277] This Note argues that a multi-dimensional, "poly-analogical" approach should be employed when assessing the fit of an exceptional technology within pre-existing doctrine. When digital information is searched, the dimensions assessed should track the three factors delineated by Roberts in *Carpenter*: (1) "the deeply revealing nature" of the information revealed, (2) the information's "depth, breath, and comprehensive reach," and (3) "the inescapable and automatic nature of [the information's] collection."[278] The *Carpenter* factors look beyond the function of the technology employed, to the nature of the information revealed by the surveillance.[279]

Part II first explores the inherently unstable nature of the Fourth Amendment. Next, it discusses what makes a technology "exceptional," requiring the Court to deviate from conventional, mono-analogical reasoning. This Part proposes that a technology is exceptional if it throws off the existing balance of Fourth Amendment power. Further, it proposes a cost-focused, "structural privacy rights" approach to determining if the existing balance has been disrupted. In short, this approach posits that if a new technology costs significantly less for the government to employ, it will likely eviscerate an implicit, non-legal right, which disrupts the constitutional balance. Further, this Part explains the flaws of mono-analogical legal reasoning, and why it cannot account for exceptional technologies. Finally, it analyzes how the Supreme Court's decisions in *Riley* and *Carpenter* considered technological exceptionalism in applying a comprehensive, poly-analogical analysis to fundamentally change Fourth Amendment jurisprudence.

Analogy Breakers: A Reality Check on Emerging Technologies, 80 MISS. L.J. 1319, 1320 (2011).

276 *See supra* Part I.C.

277 Milligan, *supra* note 275, at 1323–24.

278 Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

279 *See id.*

A. A Dynamic Fourth Amendment

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[280] The Supreme Court has recognized that the "basic purpose" of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[281] In theory, the Fourth Amendment's warrant requirement, mandating that an officer must acquire a warrant, founded on "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," acts as this critical safeguard.[282]

But, in reality, a warrantless government search or seizure can still comply with the Fourth Amendment if it falls into one of the many exceptions to the warrant requirement.[283] The label "exception" is a misnomer in this context, as warrantless searches occur more often than searches conducted pursuant to a warrant.[284] Absent more precise guidance from the founding era, the Court generally determines whether to exempt a given type of search from the warrant requirement "by assessing, on one hand, the degree to which it intrudes upon an individual's privacy and, on the other hand, the degree to which it is needed for the promotion of legitimate governmental interests."[285]

The Court's ad hoc approach to invoking the warrant requirement has thus forged hundreds of seemingly unrelated rules—frustrating scholars, judges, and citizens alike.[286] In

---

280 U.S. CONST. amend. IV.

281 Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967).

282 U.S. CONST. amend. IV.

283 *See generally* Kentucky v. King, 563 U.S. 452 (2011) (explaining that the warrant requirement is subject to reasonable exceptions).

284 Riley v. California, 134 S. Ct. 2473, 2482 (2014).

285 *Id.* at 2484.

286 In a 2009 interview, Justice Scalia discussed his hatred of Fourth Amendment cases, complaining that every case is so fact specific that a particular opinion merely answers "variation 3,542." Interview by Susan Swain with Antonin Scalia, Assoc. Justice, United States Supreme Court, in Wash. D.C. (June 19, 2009), https://www.c-span.org/video/?286079-1/supreme-court-justice-scalia [https://perma.cc/V7QW-9FZS]; *see also* Samuel C. Rickless, *The*

response to the ostensibly jumbled mess of Fourth Amendment jurisprudence, Professor Orin Kerr posits that the amendment's interpretation must constantly change with advancing technologies and social norms.[287] Professor Kerr reasons that the balance of power struck by the amendment, in any given technological and social era, is inherently unstable.[288] Thus, the amendment is constantly adjusting its scope.[289] When changing technology or social norms expand government power, the Supreme Court tightens Fourth Amendment protection; and when they threaten government power, the Court loosens constitutional protections.[290] Since technology alters how citizens commit crimes and how police catch them, new technologies threaten the balance between individual privacy and effective law enforcement by enabling both police and citizens to accomplish tasks they could not previously accomplish.[291] Judges must respond to such changes to restore the preexisting level of police power, an approach Kerr calls "equilibrium adjustment."[292]

The Supreme Court's approach to the infrared thermal imaging device at issue in *Kyllo v. United States* exemplifies Kerr's theory.[293] In *Kyllo*, police suspected that the defendant was growing marijuana inside his home using high intensity lamps.[294] Subsequently, police used a thermal imaging device, set up on a *public street*, to show that part of the defendant's home was unusually hot.[295] Police used this information to secure a warrant

---

Coherence of Orthodox Fourth Amendment Jurisprudence, 15 GEO. MASON U. C.R.L.J. 261, 261 (2005) ("If there is any statement to which virtually all constitutional scholars would agree, it is that orthodox Fourth Amendment jurisprudence is a theoretical mess, full of doctrinal incoherence and inconsistency, revealing not much more than the constitutionally unmoored ideological predispositions of shifting majorities of Supreme Court justices.").

287 Kerr, *supra* note 111, at 480.

288 *Id.* at 487.

289 *See id.* at 480.

290 *Id*. at 482.

291 *See generally id.*

292 *Id.* at 480; *see also* Ohm, *supra* note 122, at 1312 ("I embrace [equilibrium adjustment] theory as not only a convincing description of what courts have done but also a normatively desirable theory of what courts should do.").

293 533 U.S. 27 (2001).

294 *Id*. at 27.

295 *Id.* at 29–30.

to search the defendant's home, resulting in criminal charges against the defendant and a Fourth Amendment challenge to the police's warrantless use of the thermal imaging device.[296] Writing for the majority, Justice Scalia framed the inquiry at issue as: what limits must the Court place on the power of technology to avoid the evisceration of individual liberties?[297] Ultimately, the Court held that using sense enhancing technology to obtain information about the interior of the home "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search."[298] Notably, the Court reasoned that its holding "assures preservation of the degree of privacy against government that existed when the Fourth Amendment was adopted."[299] The *Kyllo* Court recognized that the police had gained an unfair advantage in determining facts due to technological innovation, and subsequently fashioned its ruling to address this imbalance and tighten Fourth Amendment safeguards.[300]

However, Kerr's equilibrium adjustment theory does not discuss the types of novel technologies that disturb the constitutional balance.[301] The following sub-part discusses the kind of technological change that disrupts the Fourth Amendment equilibrium, requiring a departure from conventional legal analysis. This Note adopts Professor Ohm's label and refers to such technologies as "exceptional."

1. Technological Exceptionalism

The idea of exceptionalism is that "a person, place, object, or concept is qualitatively different from others in the same basic

---

296 *Id.*

297 *See id.* at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance in technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

298 *Id.* at 34.

299 *Id.*

300 *See generally id.*

301 *See generally* Kerr, *supra* note 111.

category."[302] If something is "exceptional," it differs in meaningful respects from others of its kind.[303] It follows that the law should depart from conventional analysis when assessing disputes arising from the exceptional thing.[304] In departing from conventional analysis, the law should decline to analogize an exceptional thing to other "non-exceptional" things of its kind.[305]

For instance, disputes at sea are treated as exceptional. Since there is no sovereign of the open sea, the laws of tort, property, and contract provide distinct rules to resolve maritime disputes.[306] Moreover, many scholars propose that the internet, like maritime law, constitutes a separate sovereign that no contemporary legal system can adequately govern.[307] Thus, they argue that cyberspace should be treated differently, and that the law should engage in a standalone analysis when disputes arise.[308]

Ryan Calo synthesizes this viewpoint in arguing that the field of Cyberlaw is premised on the idea that fundamental advances in technology—such as the internet—are so qualitatively and quantitatively different from what has come before, that they force the law to treat them differently.[309] Calo defines a technology as exceptional, and thus requiring a standalone legal analysis, "when its introduction into the mainstream requires a systematic change to the law or legal institutions in order to reproduce, or if necessary displace, an existing balance of values."[310]

At first glance, Calo's definition seems circular, as it states: (1) if a technology is exceptional, it requires different treatment from the law; and (2) a technology will be deemed exceptional if it

---

302 Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 550 (2015).
303 *Id.* at 551.
304 *See id.*
305 *See id.* at 550.
306 *Id.* at 551.
307 *Id.*
308 *But see* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207–08 (arguing against internet exceptionalism by likening studying Internet law to studying "the law of the horse").
309 Calo, *supra* note 302, at 552.
310 *Id.*

requires the law to treat it differently.[311] However, Calo's focus is pointed toward the technology's impact on an existing balance of values—suggestive of Kerr's equilibrium adjustment theory.[312] In the Fourth Amendment context, this Note extrapolates Calo's definition to state that a technology is exceptional if its function and other attributes meaningfully disturb the existing balance of values between effective law enforcement and individual privacy.[313] If a technology is shown to disrupt the existing balance of Fourth Amendment values, it is exceptional, and should not be conventionally analogized to other technologies of its kind.[314]

2. Quantifying What Renders a Technology "Exceptional"

But, how do we *quantify* a disruption to the balance of Fourth Amendment values? Paul Ohm, in endorsing and expanding Kerr's equilibrium adjustment theory, asserts that introducing "statistical quantities," such as an empirical study showing the relative costs of police surveillance techniques,[315] could evidence that a particular surveillance technique disturbed the constitutional balance.[316] Ohm ratifies Bankston & Soltani's[317] focus on the relative costs of surveillance techniques as an acceptable metric to determine if the technique caused a constitutional imbalance.[318]

This Note explores Bankston & Soltani's cost-focused, structural privacy rights approach to determine if a new technology disrupts the Fourth Amendment. The cost-centric, structural privacy rights model is one way to lend rigor to the equilibrium

---

311 *See id.* at 552–53.
312 *See* Kerr, *supra* note 111, at 478.
313 *See infra* Part I.A.3.
314 *See* Calo, *supra* note 302, at 552–53.
315 Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 337–38 (2014).
316 Ohm, *supra* note 122, at 1313.
317 Askhan Soltani is an independent researcher and technologist specializing in privacy, security and behavioral economics. Bankston & Soltani, *supra* note 315, at 357. Kevin Bankston is an activist and attorney who specializes in the areas of free speech and privacy law. *Kevin Bankston*, NEW AM., https://www.newamerica.org/our-people/kevin-bankston/ [https://perma.cc/UJ6S-Y4VP] (last visited Jan. 31, 2019).
318 *See* Ohm, *supra* note 131, at 22.

adjustment theory, by analyzing the consequences of a relaxation of financial constraints on law enforcement. It is not the only metric that can concretize if, and the extent to which, the Fourth Amendment balance has been disrupted.

3. Cost-Centric Structural-Privacy Rights Approach to "Exceptionalism"

Bankston & Soltani theorize that a Fourth Amendment search has occurred if a new technology makes it "much less expensive" to gather information than previous technologies.[319] This proposition is underscored by Harry Surden's theory of "structural privacy rights," defined as: non-legal, implied regulations on government conduct that society has come to expect will not be infringed, due to physical and technological barriers preventing government acquisition of the information sought to remain private.[320] As technology advances, technological barriers, specifically the high costs of engaging in long-term, comprehensive surveillance, erode, allowing government access to information formerly expected to remain private.[321] As these barriers erode, individuals swiftly and permanently lose the underlying structural privacy right they once protected.[322] Surden calls the diminution in "structural" privacy rights after the advent of a new technology, a "rights-shift."[323]

Further, structural privacy *rights*, are akin to "negative legal rights"[324] that emanate from structural privacy *constraints*.[325]

---

[319] *See* Bankston & Soltani, *supra* note 315, at 337.

[320] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1608–09 (2007).

[321] *Id.*

[322] *See id.*

[323] *See id.* at 1618; Bankston & Soltani, *supra* note 315, at 339–41. Surden employs the term "rights-shift" to describe technology's erosion of a structural right resulting in a gap in the regulatory scheme constraining infringements on societally recognized expectations of privacy. *See* Surden, *supra* note 320, at 1618–19.

[324] Wesley Hohfeld defined individual legal rights in terms of how others are required to behave in relation to the rights holder. Moreover, he famously suggested that a "negative legal right" is created when others have a legal duty to refrain from behaviors that interfere with the rights holder. Joseph William

Moreover, advances in technology diminish a structural right indirectly, by removing a structural constraint.[326] Structural privacy constraints, a type of "non-legal regulatory device,"[327] arise from the practical short-comings of the current technological and physical state of the world.[328] Due to physical and technological limits, some information gathering activities will be so costly in resources and time, that they are effectively impossible to regularly execute.[329] The presence of these costs implicitly curtail the behavior of law enforcement seeking such private information—by acting as a structural *constraint* on police behavior.[330] In turn, society comes to expect that law enforcement will not engage in certain behaviors; conferring on them an expectation based, "negative structural right."[331]

Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 WIS. L. REV. 975, 986–87.

[325] A structural privacy constraint can be seen to confer the structural privacy right. There is a parallel between a non-legal constraint mechanism, caused by practical limitations, and a legal right, created by judge or legislature, in that they both provide citizens with the same protection. In support of this proposition, Harry Surden, Fellow at the Stanford Center for Computers and the Law, posits that legal rights are created when others have a legal duty to refrain from behavior that interferes with the rights-holder. It follows from this definition that such a right would limit interference with a right-holder's protection. The same outcome, limited interference with a rights-holder' protection, is achieved through non-legal constraint mechanisms. Surden further emphasizes that non-legal constraint mechanisms may give rise to relationships between constraints and behaviors that are functionally equivalent to the relationships giving rise to legal rights. *See* Surden, *supra* note 320, at 1610–20.

[326] *Id.*

[327] "Non-legal regulatory devices" are also known as "alternative behavior regulators." *Id.* at 1610.

[328] There are two types of structural constraints—explicit and latent. Latent structural constraints—which are more applicable to regulating private information—are the secondary costs arising from the current technological or physical state of the world. Put differently, the limitations of technology make some behaviors too timely or expensive to be conducted on a regular basis. *Id.* at 1613. By contrast, an explicit structural constraint is an overt constraint on a behavior. The paradigm example of an explicit structural constraint is a physical fence surrounding a property. In that scenario, a certain behavior—entering the property—is constrained by the physical cost incurred by climbing over the fence. *Id.* at 1612.

[329] *See generally id.*

[330] *See id*. at 1614.

[331] *Id.*

For example, in *Kyllo*, the Court recognized that sense enhancing technology disrupted the status quo between police and citizens, because it gave police "x-ray vision" inside a suspect's home, which was unavailable before the advent of thermal imaging technology.[332] Thus, the "negative structural right" to be free from long-distance surveillance of the interior of one's home was eroded by the advent of thermal imaging, thereby disrupting the Fourth Amendment balance.

Structural privacy protections are especially important in the field of privacy law.[333] Justice Alito remarked in his concurrence in *Jones*, that before the advent of the computer, "the greatest protections of privacy were neither constitutional nor statutory, but practical."[334] Scholars thus assert that as structural privacy rights erode in the face of new technology, individual privacy protections are greatly diminished.[335] Moreover, the implicit nature of a structural right renders it of little interest to policy makers: "[i]n other words, as long as some mechanism is acceptably constraining unwanted behavior, the underlying issue and the choice of mechanism will garner little attention."[336] Since it is easy for policy makers to overlook "rights-like" relationships that are not expressed by law, legislators focus little energy on codifying structural rights into legal ones.[337] Thus, a structural right will rarely, if ever, be accompanied by a legal right conferring the same protection.[338] Therefore, when a structural right dissolves, society is left with no regulation of the formerly curtailed behavior; resulting in a sharp shift in the regulatory framework.[339] Harry Surden terms this phenomenon a "rights-shift."[340]

---

[332] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[333] *See* United States v. Jones, 565 U.S. 400, 418–31 (2012) (Alito, J., concurring).

[334] *See id*. at 429.

[335] *See* Surden, *supra* note 320, at 1617; Ohm, *supra* note 131, at 59.

[336] Surden, *supra* note 320, at 1614.

[337] *See id.*

[338] *See id.*

[339] Once a particular constraint mechanism is successfully "employed"—such as a structural privacy constraint—policymakers may be unaware or indifferent to the details of the regulatory mechanism as long as it reasonably constrains unwanted behavior. *See id.* "In other words, as long as some mechanism is

Justice Alito's concurrence in *Jones* serves as a helpful example of the Court's recognition of the swift disappearance of a structural privacy right—the right to be free of comprehensive, long term location tracking.[341] The Court explicitly noted that "society's expectation has been that law enforcement agents and others would not—and indeed simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[342]

4. Cost Centric Approach to Eroding Privacy Rights

In his concurrence in *Jones*, Justice Alito adopts a cost-centric approach to the disappearance of the structural right at issue.[343] First, he discusses the financial constraints that rendered "traditional surveillance for any extended period of time [] difficult[,] costly, and [] rarely undertaken."[344] Alito explains that comprehensively monitoring an individual over an extended period of time, "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," a costly undertaking that would have only been justified for an unusually important investigation.[345] Alito jokes that such comprehensive monitoring would not have been impossible in the Framer's era absent "a very tiny constable . . . with incredible fortitude and patience" to hide for twenty-eight days.[346] After noting that devices like GPS surveillance "make long-term monitoring relatively easy and cheap,"[347] removing the structural constraint on comprehensive, long-term monitoring, Alito recognizes the need for a legal constraint to restore constitutional balance. Thus, Alito maintains

---

acceptably constraining unwanted behavior, the underlying issue and the choice of mechanism will garner little [legal] attention." *Id.*

340 *Id.* at 1618.

341 *See* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

342 *Id.*

343 *See id.* at 429.

344 *Id.*

345 *Id.*

346 *Id.* at 420 n.3.

347 *Id.* at 430. After *Jones*, Bankston & Soltani determined that GPS surveillance costs twenty-eight times less than tracking an individual via covert car pursuit, and tracking via CSL costs half as much as GPS surveillance. *See* Bankston & Soltani, *supra* note 315, at 350.

that even if the government had not physically trespassed on the defendant's car, Jones had a reasonable expectation of privacy over the totality of his movements; based on a long-held expectation that law enforcement would not, and could not, access such information.[348] Here, Alito has recognized a rights-shift disrupting the Fourth Amendment equilibrium, caused by the advent of GPS.[349] Under the framework proposed by this Note, Alito implicitly deemed GPS technology "exceptional."

Bankston & Soltani add a quantitative metric to lend rigor to Alito's "structural rights-shift" theory of GPS technology, at issue in *Jones*.[350] To do so, they conducted an empirical study, assessing the relative expense to law enforcement of employing: foot pursuit, covert pursuit, single car pursuit, five car pursuit, beeper technology, cell-phone tracking using a sting ray, GPS tracking, and tracking via CSLI.[351] After comparing the relative costs of these techniques, they assert a general rule of thumb: if a new technology makes it "much less expensive" to collect information about individuals, a rights-shift has occurred.[352] This paradigm proposes a cost-centric approach to determining technological exceptionalism.[353] If a technology makes surveillance "much less expensive;" a rights-shift will ensue; tipping the Fourth Amendment balance in favor of law enforcement; which, under the definition proposed by this Note, renders the technology exceptional.[354]

To continue, Ryan Calo and Paul Ohm propose that if a technology is exceptional, it should receive a "fresh default analysis" or "standalone."[355] Since many new technological advances cause a rights-shift, throwing off the balance of power struck by the Fourth Amendment, this Note argues that courts will be wary to employ a fresh-default analysis each time an

---

348 *See Jones*, 565 U.S. at 430 (Alito, J., concurring).
349 *See* Surden, *supra* note 320, at 1626.
350 Bankston & Soltani, *supra* note 315, at 337.
351 *See id* at 342.
352 *Id.* at 337.
353 *See id.*
354 *Id.*; Ohm, *supra* note 131.
355 Ohm, *supra* note 131, at 47; *see* Calo, *supra* note 302, at 551.

exceptional technology is at issue. Instead, this Note endorses a holistic analysis of the technology and its implications, geared toward the class of information sought. This approach does not automatically reject well-settled Fourth Amendment doctrine, but allows for a departure from categorical rules in certain circumstances. The following sub-part discusses this holistic analysis, labeled by Professor Luke Milligan as "poly-analogical" reasoning.

B. Rejecting Conventional Analogies When an Exceptional Technology Is at Issue

Analogical reasoning is often thought to be at the core of legal reasoning, and thus, judicial decision making.[356] An "analogy" is defined as "the inference that two or more things that are similar to each other in some respects are also similar in other respects."[357]

1. Mono-Analogical Reasoning

The prevailing approach courts use to analogize a novel fact pattern to a pre-existing one is described by Professor Milligan as mono-analogical.[358] The term mono-analogical describes a type of analogical reasoning where only one dimension of a tool or technology is assessed.[359] When technology is analyzed, most often, the technology's function is assessed by comparing it to the function of a previous technology.[360] Mono-analogical reasoning typically works in "four simple steps:"

(1) Fact pattern A has a certain characteristic, X; (2) Fact pattern B differs from A in some respects, but shares characteristic, X; (3) the law treats characteristic X in a certain way; (4) because B shares a characteristic (X) with A, the law should treat B the same way it treats A.[361]

---

356 *See* Grant Lamond, *Precedent and Analogy in Legal Reasoning*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2016); Edward H. Levi, *An Introduction to Legal Reasoning*, 15 U. CHI. L. REV. 501, 504 (1948).
357 *Analogy*, BLACK'S LAW DICTIONARY (2d ed. 1995).
358 Milligan, *supra* note 275, at 1319–20.
359 *Id.* at 1323–24.
360 *See id.* at 1322.
361 *Id.* at 1321–22.

Mono-analogical reasoning can be very useful when used to liken two non-exceptional items, regardless of any facial similarities between them.[362] For example, the facts of the famous tort case *MacPherson v. Buick Motor Co.*, in which a car manufacturer was held liable for damages suffered by a third-party, can be analogized to a situation where a plaintiff finds a dead snail at the bottom of her soft drink; based on only one element of each factual scenario.[363] A soda bottle and a car are quite different. However, the legal nexus between the two—the fact that negligent production of either can be expected to produce "danger"—is strong enough to determine that both scenarios allow a plaintiff to directly sue a manufacturer.[364] Here, the Court only needed to focus on one dimension of each fact pattern to reach its conclusion: if a soda bottle or a car are negligently manufactured, injury to a third-party, not in contract with the manufacturer, may result.[365] The mono-analogical reasoning employed here may look as follows:

> (1) A negligently manufactured vehicle can be expected to produce "danger" to its user; (2) A negligently produced soda bottle (for example, one with a snail inside) may also produce danger to its user; (3) the law will hold a manufacturer liable to an injured user if a vehicle malfunctions due to its manufacturer's negligence; (4) because a user may be injured by a snail negligently allowed in a soda bottle, the law will hold the manufacturer liable if the user is injured.[366]

---

[362] Frederick Schauer & Barbara A. Spellman, *Analogy, Expertise, and Experience*, 84 U. CHI. L. REV. 249, 262 (2017).

[363] MacPherson v. Buick Motor Co., 111 N.E. 1050, 1055 (N.Y. 1916); Donoghue v. Stevenson [1932] AC 562 (HL) 562.

[364] *See* Schauer & Spellman, *supra* note 362, at 263–64.

[365] *Id.*

[366] *Cf. id.* (this type of mono-analogical reasoning looks only at the product's propensity, if negligently manufactured, to cause injury to a user not in contract with the product's manufacturer. Thus, although there are many facial differences between a tortuously manufactured car and soda bottle, courts often reach conclusions based a single similarity between otherwise dissimilar cases.)

In this instance, the dimensions that differentiate a car and soda bottle manufacturer, such as the tools used for manufacturing, customers reached, efficiency of the operation, and so on, do not affect the relevant legal analysis. The Court reached its conclusions, focusing on just one aspect of the manufacturers: does their product, if produced negligently, have the potential to cause danger to a user?[367]

By contrast, mono-analogical reasoning is under-inclusive when an exceptional technology is analyzed to a non-exceptional one. A famous example of the Court attempting to draw such an analogy occurred in *Olmstead v. United States*.[368] In *Olmstead*, FBI agents installed wiretaps in the basement of the defendant's office building and in the streets near his home due to suspicion that he was illegally transporting liquor.[369] The Court addressed whether the wiretaps constituted a warrantless "search" of the defendant's conversations, despite the lack of government trespass. Finding that no search occurred, the Court analyzed as follows:

> (1) Numerous cases before the Court involved fact patterns without physical trespass; (2) the Court had never found a Fourth Amendment search without physical trespass; (3) the FBI's use of a wiretap did not involve physical trespass; (4) the use of a wiretap does not constitute a Fourth Amendment search.[370]

Olmstead, which was overturned by *United States v. Katz* in 1967, is a prime example of the Court's failure to recognize the exceptional nature of the wiretap in its ruling. Electronic eavesdropping, first employed by law enforcement in the 1890s, disrupted the balance of Fourth Amendment protection by allowing law enforcement access to information it was unable to previously retrieve without a warrant.[371] However, it took the Supreme Court

---

367 *See id.*

368 *See* Olmstead v. United States, 277 U.S. 438, 464 (1928).

369 *Id.* at 457.

370 *See* Milligan, *supra* note 275, at 1323.

371 William Lee Adams, *Brief History: Wiretapping*, TIME (Oct. 11, 2010), http://content.time.com/time/magazine/article/0,9171,2022653,00.html [https://perma.cc/6C4U-DRVX]; Michael Pollack, *A Short History of*

another seventy years to properly tighten Fourth Amendment scrutiny to account for this imbalance.[372]

To continue, in cell-phone cases before 2014, only one dimension of a smart-phone—its functionality—was typically discussed.[373] Since cell-phones disrupted the Fourth Amendment equilibrium, rendering them exceptional,[374] engaging in an analysis solely focused on their function is gravely under-inclusive.

Further, in the context of the *Riley* case, if the Court applied a mono-analogical approach, premised on the idea that a cell phone *functions* like an address book or other pre-digital tool, a warrantless search incident to arrest would be lawful.[375] Moreover, in the context of the *Carpenter* case, if CSLI records functioned as business records, like the bank records at issue in *Miller*, their warrantless search would be lawful under the third-party doctrine.[376]

2. Poly-Analogical Reasoning

To combat the under-inclusiveness of mono-analogical reasoning, this Note proposes that courts employ a holistic, "poly-analogical" approach. Such an approach invites courts to reflect on the practical implications of a new technology, beyond its mere function. A technology's non-functional dimensions may include frequency of use, storage capacity, efficiency, and ability to

---

Wiretapping, N.Y. TIMES (Feb. 28, 2015), https://www.nytimes.com/2015/03/01/nyregion/a-short-history-of-wiretapping.html [https://perma.cc/PNW2-KMH5].

372 *See* Katz v. United States, 389 U.S. 347, 353 (1967) (overruling *Olmstead*).

373 See People v. Diaz, 244 P.3d 501, 507–08 (Cal. 2011), *abrogated by* Riley v. California, 134 S. Ct. 2473 (2014) ("[N]either defendant nor the dissent persuasively explains why the sheer quantity of personal information should be determinative. Even 'small spatial container[s]' that hold less information than cell phones may contain highly personal, intimate and *private* information, such as photographs, letters, or diaries.").

374 *See infra* Part I.C.

375 Riley v. California, 134 S. Ct. 2473, 2485 (2014); *cf.* United States v. Runyan, 290 F.3d 223, 236 (5th Cir. 2002) (analogizing the search of floppy disks and CDs to opening a closed container). *See generally* Milligan, *supra* note 275.

376 *See generally* Milligan, *supra* note 275.

aggregate information.[377] Justice Roberts, in *Carpenter*, delineated three non-functional factors to help guide a court assessing the role of an exceptional technology in pre-existing doctrine.[378] These factors are aimed not at the technology's function, but the nature of the information targeted.[379]

The following sub-part will discuss the Court's poly-analogical approach to smart-phone cases in *Riley* and *Carpenter*. Although Justice Roberts did not specifically address the three aforementioned factors until *Carpenter*, they were eluded to, and guided the Court's reasoning, in *Riley*.

3. *Riley*, *Carpenter*, and Poly-Analogical Analysis in Action

Chief Justice Robert's reasoning in *Riley* and *Carpenter* exemplify the Court's response to technological exceptionalism, and its attempt to restore the Fourth Amendment to a state of equilibrium.[380] To elaborate, the Court first identified the exceptional nature of the technology at issue by assessing its impact on the balance of power between police and individual privacy. Then it rejected conventional analogies in light of the technology's exceptionalism, focusing on both the function of the smart-phone on its non-functional dimensions. Finally, it engaged in a holistic analysis to ascertain the propriety of applying the search incident to lawful arrest and third-party doctrines to a smart phone, and CSLI, respectively.[381]

4. *Riley* Declines to Extend the Search Incident to Lawful Arrest Doctrine to a Smart Phone on Arrestee's Person

A poly-analogical approach was employed by Justice Robert's in the majority opinion of *Riley*.[382] In *Riley*, the government attempted to analogize searching an arrestee's cell phone to

---

377 *Id.* at 1320.

378 Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (emphasizing (1) "the deeply revealing nature" of the information retrieved, (2) the information's "depth, breadth, and comprehensive reach," and (3) "the inescapable and automatic nature of its collection").

379 *See id.*

380 *See generally Carpenter*, 138 S. Ct. 2206; *Riley*, 134 S. Ct. 2473.

381 *See* cases cited *supra* note 380.

382 *See Riley*, 134 S. Ct. at 2485.

searching a carton of cigarettes, address book, wallet, or purse, incident to arrest.[383] Roberts sternly rejected this argument, holding that inspecting the contents of an arrestee's pockets does not substantially intrude on an arrestee's privacy beyond the arrest itself when a *physical item* is searched, but, "any extension of that reasoning to digital data has to rest on its own bottom."[384] Moreover, Roberts analyzed a cell phone's non-functional dimensions, ultimately rejecting the government's attempt to liken a smartphone to pre-digital items.

First, a cell phone has immense storage capacity.[385] A cell-phone can store the equivalent of "millions of pages of text," dating back to the purchase of the phone, or even earlier.[386] Next, cell-phone data can be aggregated.[387] A cell phone collects in one place many distinct types of information—"an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record."[388] Additionally, the Court discussed the pervasive nature of the smart phone.[389] "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day."[390] However, as of 2013, nearly three quarters of smart phone users reported being within five feet of their phones most of the time, while 12% of users admitted to using their phones in the shower.[391] Justice Roberts sarcastically notes that "[cell phones] are now such a pervasive and insistent part of daily life that the proverbial visitor

---

383 In *Riley*, the government argued that searching all the data on an arrestee's cell phone was "materially indistinguishable" from searches of physical items such as an address book, wallet, or purse. Justice Roberts, in response, reasoned that "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Id.* at 2488.

384 *Id.* at 2489.

385 *Id.*; *see* Milligan, *supra* note 275, at 1320.

386 *Riley*, 134 S. Ct. at 2489.

387 *See id.*

388 *Id.*

389 *Id.* at 2490.

390 *Id.*

391 *Id.*

from Mars might conclude they were an important feature of human anatomy."[392]

The *Riley* Court expressly rejected both the government's proposed mono-analogical approach,[393] and the previously categorical rule of *United States v. Robinson* that a warrantless search incident to arrest is presumptively lawful.[394]

5. *Carpenter* Declines to Extend the Third-Party Doctrine to CSLI Held by a Private Wireless Carrier

Chief Justice Roberts, in his majority opinion, isolates three specific factors to help guide a court's analysis of an exceptional technology.[395] To begin, the Court explained that information that is "deeply revealing" of some private quality of the person under surveillance warrants protection.[396] Quoting Justice Sotomayor's concurrence in *Jones*, the Court addressed how location information reveals more than someone's movements, but through them, the individual's "familial, political, professional, religious, and sexual associations."[397] This factor highlights the connection between the intimate nature of the data at issue, and a person's Fourth Amendment right over that data.[398] The *Carpenter* Court found that time stamped CSLI, similar to GPS information, provided an intimate window into a person's life and was thus,

---

[392] *Id.* at 2484.

[393] "And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form. . . . [I]t is implausible that [a citizen] would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets. But because, each of those items has a pre-digital analogue, [the government argues] police…would be able to search a phone for all those items—a significant diminution of privacy." *Id.* at 2493.

[394] United States v. Robinson, 414 U.S. 218, 224 (1973).

[395] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[396] *Id.*

[397] *Id.* at 2217.

[398] The connection between the intimacy of information and one's expectation of privacy over the information is not new. Professor Orin Kerr's "private facts" model of Fourth Amendment protection centers on the sensitivity and intimacy of the information obtained. Freiwald's intrusiveness factor also determines the intimacy of the information revealed by the surveillance technique at issue. *See* Ohm, *supra* note 131, at 14.

"deeply revealing."[399] This factor, which is arguably the most important,[400] considering the Court held that CSLI "hold[s] for many Americans the 'privacies of life,'" cut in favor of finding a search had occurred.[401]

The second factor highlights the Court's willingness to protect information that possesses "depth, breadth, and comprehensive reach."[402] Professor Ohm breaks this requirement down into three discrete measures.[403] "Depth" refers to the detail and precision of the information stored.[404] "Breadth" refers to the frequency and length of data collection.[405] Finally, "comprehension" refers to the number of people tracked by the database.[406]

The Court found that CSLI possessed depth, breadth, and a comprehensive reach, emphasizing that CSLI contains "the whole of [a person's] physical movements" and a "detailed chronicle of a person's physical presence."[407] The depth factor, similar to the "deeply revealing" factor cut in favor of finding the Fourth Amendment was implicated, due CSLI's precision.[408] Since CSLI can place an individual inside a place of worship, a storefront, their home, and other revealing locations, the "depth" factor cuts toward the need for a warrant.[409]

Additionally, CSLI is invasive due to its breadth.[410] The database at issue in *Carpenter* stored "an average of 101 data points" daily, and, most wireless carriers store CSLI for five years.[411] Roberts emphasizes this point in discussing how a person may be effectively "tailed," far before law enforcement has any

---

399 *Carpenter*, 138 S. Ct. at 2217, 2223.
400 Ohm, *supra* note 131, at 13.
401 *See id.*
402 *Carpenter*, 138 S. Ct. at 2223.
403 Ohm, *supra* note 131, at 14–15.
404 *Id.* at 15.
405 *Id.*
406 *Id.*
407 *Carpenter*, 138 S. Ct. at 2219–20.
408 *See id.*
409 *See id.*
410 *See id.* at 2223.
411 *Id.* at 2209, 2218.

suspicion that they have committed a crime.[412] He notes that "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment."[413]

As for comprehensive reach, the Court determined that, since "location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."[414]

Finally, the Carpenter majority looked to the "inescapable and automatic nature" of how the information is collected.[415] This factor can also be split into two discrete inquiries.[416] First, the Court looked to the whether the surveillance was "inescapable."[417] The majority implicitly embraced petitioner's argument that cellphones have become such a pervasive part of modern life that their use cannot be considered "voluntary,"—or put differently, "escapable."[418] Whether one needs to use the service at issue "to be a functioning member of modern society" speaks to one of the underlying theories of the third-party doctrine—the extent to which the target of collection voluntarily exposed such information to a private party.[419] The majority in *Carpenter* determined this factor cut in favor of protection. Citing *Riley*, the Court held that cell phones are "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern

---

412 *Id.* at 2218.
413 *Id.*
414 *Id.*
415 *Id.* at 2223.
416 Ohm, *supra* note 131, at 19.
417 *See id.* at 19–21.
418 Brief for Petitioner, at 39–42, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).
419 *Carpenter*, 138 S. Ct. at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements.").

society."[420] Thus, a cellphone user cannot be said to voluntarily assume the risk of turning over their location data to a service provider in a meaningful way.[421]

In contrast to inescapability, the automatic nature of a surveillance method corresponds to an individual's ability to "opt-out" of having their data collected.[422] CSLI is automatic because location records are generated whenever an individual uses their phone, and there is no ability for the user to "opt-out" of having their location chronicled.[423]

III. ASSESSING HASH-VALUE MATCHING AND THE PRIVATE AND BINARY SEARCH DOCTRINES AFTER *CARPENTER*

> *"When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."*[424]

As discussed above, a technology is exceptional if it is qualitatively different from others in the same general category.[425] To determine technological exceptionalism, this Note asks

---

[420] *Id.* at 2210; *see also* Riley v. California, 134 S. Ct. 2473, 2484 (2014). Unlike the bugged container in Knotts or the car in Jones, a cell phone—almost a "feature of human anatomy,"—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. *Id.* at 2490 (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

[421] *See Carpenter,* 138 S. Ct. at 2220.

[422] Ohm, *supra* note 131, at 20.

[423] *Id.* "[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." *Carpenter*, 138 S. Ct. at 2220.

[424] *Carpenter*, 138 S. Ct. at 2222.

[425] *See supra* Part I.A.

whether, in relation to other surveillance techniques in the same category, hashing meaningfully disrupts the balance of power between law enforcement and individuals.

Positing that hashing belongs to the general category of techniques that authenticate data in the binary, this Part first assesses whether hashing makes binary authentication of data "much less expensive" than other techniques of its kind—specifically, canine sniffs and narcotics field tests. If this question is answered in the affirmative, this Note will conclude that hashing causes a rights-shift; which meaningfully disrupts the current balance of Fourth Amendment power. Moreover, if determined to be exceptional, this Note proposes that courts should decline to analogize hashing to pre-digital technologies, and instead employ a holistic analysis of hashing's functional and non-functional attributes when assessing its fit within established doctrine.

A. Surveillance Techniques that Reveal Information in the Binary

Hash-value matching to detect contraband falls into the category of surveillance techniques that reveal only the presence (or absence) of contraband. This Section explores two commonly used binary authentication techniques. First, it assesses law enforcement's use of canine sniffs, at issue in the *Place* line of cases.[426] Second, it analyzes field tests for narcotics, at issue in *Jacobsen* and its progeny.[427]

1. Canine Sniffs

Canines are widely used "volatile organic compound"[428] detectors, often employed to detect the presence of narcotics and

---

[426] *See* Illinois v. Caballes, 543 U.S. 405, 408 (2005); Indianapolis v. Edmond, 531 U.S. 32, 35 (2000); United States v. Place, 462 U.S. 696, 707 (1983); *see also supra* Part I.C.4.

[427] *See* United States v. Jacobsen, 466 U.S. 109, 112 (1984).

[428] A compound is described as "volatile" if it evaporates easily, releasing molecules into the atmosphere. *What Is a Volatile Organic Compound*, ION SCI., https://www.ionscience.com/wp-content/uploads/2019/02/What-is-a-VOC-TOFU-V1.0-UK.pdf [https://perma.cc/PTJ4-8JF8] (last visited Jan. 31, 2019).

explosives.[429] Many illicit substances, including amphetamines, cocaine, and heroin release compounds into the air that a properly trained canine can detect.[430] Upon detecting the compound, the canine will alert their handler to where it smells the drug.[431] Canines are recognized as the most mobile, flexible, fast, and durable real-time detectors of narcotics and explosives.[432]

However, canine sniffs are quite costly, for several reasons. First, they are fallible, leading to false positives. The detection of a false positive is costly because it requires further testing and subsequent litigation. The accuracy of a canine sniff is measured by both the proportion of correct "hits," (when a canine detects the presence of a drug), and the proportion of "false alerts," (when the canine incorrectly indicates the presence of a drug).[433] A perfectly

---

[429] Tadeusz Jezierski et al., *Information-Seeking Behaviour of Sniffer Dogs During Match-to-Sample Training in the Scent Lineup*, 39 POLISH PSYCHOL. BULL. 71, 71 (2008).

[430] *See generally* Ed Grabianowski, *How Police Dogs Work*, HOWSTUFFWORKS (May 3, 2004), https://people.howstuffworks.com/police-dog.htm [https://perma.cc/R54A-N9K3] (describing the process of training canines, whose sense of smell is almost fifty times as sensitive as a human's, to ferret out various narcotics); *cf.* Tadeusz Jezierski et al., *Efficacy of Drug Detection by Fully Trained Police Dogs Varies by Breed, Training Level, Type of Drug, and Search Environment*, 237 FORENSIC SCI. INT'L 112, 114 (2014) (comparing the relative ease with which trained dogs can detect marijuana, amphetamine, cocaine, and heroin). Police dogs are typically trained by first being presented with a white, odorless towel. After the dog has played with the towel, and views it as a toy, its handler will wrap an illicit substance inside the towel. The dog will then begin to associate the smell of the substance with its toy. After this, the handler will hide the towel, with the substance, in various places. When the dog smells its toy—the substance—it will dig and scratch at the area to alert its handler that it has found its toy. Grabianowski, *supra* note 431, at 4.

[431] Karl Smallwood, *How Do They Train Drug Sniffing Dogs?,* TODAYIFOUNDOUT (Jan. 19, 2018), http://www.todayifoundout.com/index.php/2018/01/how-do-they-train-drug-sniffing-dogs/ [https://perma.cc/73FJ-F9RD]. Once a dog has learned to successfully seek out a smell when commanded, the trainer conditions the dog to engage in an appropriate action to alert him to the smell. *Id.* For example, some drug detecting dogs are trained to paw at the spot where the illegal substance is located. *Id.*

[432] *See, e.g.*, Jezierski et al., *supra* note 430, at 112; Burkhard Bilger, *Beware of the Dogs*, NEW YORKER (Feb. 27, 2012) https://www.newyorker.com /magazine/2012/02/27/beware-of-the-dogs [https://perma.cc/8UFX-CB4N].

[433] *Id.* at 113.

accurate canine sniff would guarantee that no target material remains undetected, and no other materials than the target are falsely indicated by the canine.[434]

A canine may not be able to detect contraband for a variety of reasons. First, canines are not always trained in similar enough circumstances to the ones they encounter in the real world.[435] For example, a canine who can detect as little as a trillionth of a gram of a narcotic in a spare basement room, will likely not produce the same results in a crowd of people, a windy environment, or if the narcotic is moving with an individual.[436] Moreover, a canine may not be able to get close enough to the target material to detect its presence—especially if the target is moving. Additionally, canines tire out.[437] A canine that is overheated, or panting for another reason, has a less reliable nose.[438] A 2013 study involving 1219 canines showed that canines missed target material 5% of the time amphetamine was sought; 12.6% of the time cocaine was sought; and 12% of the time heroin was sought.[439]

False alerts occur due to the aforementioned fallibilities of the canines, as well as errors by handlers, and the pervasive contamination of currency by cocaine.[440] In rejecting evidence that a canine detected narcotics on a defendant, courts have noted that "a substantial portion of United States currency . . . is tainted with sufficient traces of controlled substances to cause a trained canine

---

434 *See id.*

435 Alexandra Horowitz, *The Limits of Detection*, THE NEW YORKER, https://www.newyorker.com/news/news-desk/the-limits-of-detection [https://perma.cc/YGX3-HHGT] (Apr. 24, 2013).

436 *Id.*

437 *See id.*

438 *Id.*

439 Jezierski et al., *supra* note 430, at 114. The above results come from a 2013 study conducted by the Institute of Genetics and Animal Breeding of Polish Academy Sciences, Department of Animal Behavior. The trial included 1219 experimental searching tests; 440 were performed by German Shepherds, 517 by Labrador retrievers, 203 by Terriers, and 59 by Cocker Spaniels. On a single day, no more than two searching tests were conducted by any dog. If two searching tests were conducted on a specific day for one dog, the second test was done in a separate room. The dogs and their handlers waited in another building until they were asked to come in for their trial. *Id.*

440 Illinois v. Caballes, 543 U.S. 405, 411–12 (2005) (Souter, J., dissenting).

to alert to their presence" and because as much of 80% of all currency in circulation contains drug residue, a dog alert is of "little value."[441]

Additionally, it is expensive for law enforcement to train and use canines. It costs law enforcement about $15,000 to train a team of fourteen canines.[442] Purchasing a single trained canine will cost between $5,000 and $25,000.[443] These metrics do not even consider the cost of paying the handler's salary—who will often have to work early mornings and late nights to continuously train the canine.[444]

2. Narcotics Colorimetric (Spot) Test

Chemical field tests are an "illicit drug identification technique commonly used by law enforcement, border security personnel, and forensic laboratories" to detect the presence of narcotics.[445] Suspected illicit materials seized by police are often analyzed on the spot to determine if an illegal drug is present.[446] Although the government uses a range of analytical techniques to determine the existence of narcotics, the most commonly used is a colorimetric ("spot") test.[447] During a spot test, an examiner adds a chemical

---

[441] United States v. $242,484.00, 351 F.3d 499, 511 (11th Cir. 2003) (noting that because as much as 80% of all currency in circulation contains drug residue, a dog alert "is of little value"), *vacated on other grounds by reh'g en banc*, 357 F.3d 1225 (11th Cir. 2004); *see also* United States v. Carr, 25 F.3d 1194, 1214–17 (3d Cir. 1994) (Becker, J., concurring in part and dissenting in part) ("[A] substantial portion of United States currency . . . is tainted with sufficient traces of controlled substances to cause a trained canine to alert to their presence."); *Caballe*s, 543 U.S. at 412.

[442] Michael Von Fremd, *Intense Training for Bomb-Sniffing Dogs*, ABC NEWS (Jan. 12, 2012) https://abcnews.go.com/WNT/story?id=130545&page=1 [https://perma.cc/3545-3ZCE].

[443] *How Do You Train a Dog to Sniff Bombs?*, PRICEONOMICS (Dec. 31, 2015), https://priceonomics.com/how-do-you-train-a-dog-to-sniff-bombs/ [https://perma.cc/2YYA-M2NC].

[444] *Id.*

[445] Morgan Philp & Shanlin Fu, *A Review of Chemical 'Spot' Tests: A Presumptive Illicit Drug Identification Technique*, 10 DRUG TESTING & ANALYSIS 95, 95 (2018).

[446] *Id.*

[447] *Id.* Further, pursuant to evidentiary authentication requirements, a positive spot test will be followed by laboratory testing using a more precise method,

reagent to a sample of the seized material and observes any changes in color. Specified color changes indicate the presence of a particular class of compounds—such as amphetamines.[448]

A 2018 study by the National Institute of Justice ("NIJ") indicated that the average total cost of performing a color spot test is $166.98 per sample tested.[449] Moreover, the National Criminal Justice Reference Service is proposing the introduction of portable mass spectrometric instruments, which are more precise than the current spot tests, and would cut costs by ensuring only probative samples are re-tested in the laboratory.[450]

However, despite the relatively low costs of narcotics spot tests, they have a high error rate, resulting in subsequent litigation and retesting costs.[451] Additionally, more precise methods are far more expensive and timely to employ.[452] Color tests are imperfect because of their inherently subjective nature.[453] A police officer, with just hours of training from another officer who knows the

---

such as chromatography or mass spectrometry. Prasant Potuluri, *Drug Identification in Law Enforcement*, EVIDENCE TECH. MAG., http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1260&Itemid=49 [https://perma.cc/87EJ-PQM2] (last visited Jan. 31, 2019).

448 Philp & Fu, *supra* note 445, at 96.

449 Christopher C. Mulligan et al., *Analytical Validation and Impact Assessment of On-Site Evidence Screening via Ambient Sampling*, *Portable Mass Spectometry,* NAT'L CRIM. JUST. REFERENCE SERV. 8 (2018), https://www.ncjrs.gov/pdffiles1/nij/grants/251910.pdf [https://perma.cc/396J-FN4E]. This metric includes the on-site, precinct, transportation, in-laboratory, and fixed costs of testing a single sample. *Id.*

450 *Id.* at 9–10.

451 *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 412 (2005) (Souter, J., dissenting) ("[t]he infallible dog [] is a creature of legal fiction. . . . [T]heir supposed infallibility is belied by judicial opinions describing well-trained animals sniffing and alerting with less than perfect accuracy, whether owing to errors by their handlers, the limitations of the dogs themselves, or even the pervasive contamination of currency by cocaine.)

452 *See id.* at 56. The cost of a mass spectrometer, the most precise way to test for narcotics, can cost up to $1,000,000. *Id.* at 54 (graphing the relative costs of various analytical techniques to detect narcotics and determining color spot tests are the least costly method, but also the least accurate).

453 *See id.* at 60.

technique, can perform a spot test and determine its result.[454] Further, these tests are only done when law enforcement believes the substance they are testing is illicit. Thus, the tests are always done in anticipation of criminal litigation—which makes their subjective nature more worrisome. In addition, although color tests can identify the most common drugs of abuse, there are limitations on what can be detected.[455] Color tests can only identify previously characterized drugs, which creates an issue due to the growing number of new psychoactive substances ("NPS").[456] There are a significant number of NPS on the market, including Fentanyl and other synthetic opioid derivatives, that color testing cannot identify.[457]

B. Hash-Value Matching is Exceptional

Hash-value matching is qualitatively different from other types of binary authentication, such as canine sniffs and spot tests.[458] Other types of binary authentication methods are conducted *after* the government has an articulable suspicion of criminal wrongdoing.[459] Alternatively, every internet communication is hashed, without any suspicion.[460] Second, hashing is conducted by a private entity, at no cost to the government.[461] Under Bankston and Soltani's theory, it is thus much less costly than other methods of its kind.[462] Therefore, the collection of hash-evidence causes a

---

[454] *See id.* There have been significantly more NPS on the market, shown by a statistic from the EU that a NPS was reported to their Early Warning System every week in 2016. Fentanyl and other synthetic opioid derivatives remain extremely dangerous public safety threats, particularly in the United States where 167 kilograms of illicit fentanyl was seized in 2015. Other seized substances include tryptamines, anesthetics, steroids, benzodiazepines, and hallucinogens. Philp & Fu, *supra* note 445, at 95.

[455] Philp & Fu, *supra* note 445, at 95.

[456] *Id.*

[457] *See id.*

[458] *See supra* Part I.A.

[459] *See, e.g.,* United States v. Jacobsen, 466 U.S. 109, 111–12 (1984); United States v. Place, 462 U.S. 696, 698 (1983).

[460] *See supra* Part I.A.

[461] *See supra* Part I.A.

[462] *See generally* Bankston & Soltani, *supra* note 315, at 350–56. *Compare id. with* Parts III.A.1–III.A.2 (discussing how a colorimetric spot test costs approximately $166—without accounting for subsequent testing and litigation

rights-shift and erodes a structural right to be free from pervasive monitoring.[463] This rights-shift tips the Fourth Amendment balance toward the government. Hashing is thus an exceptional technology which "supports a break with judicial precedent."[464]

1. Hashing is Non-Targeted

The fundamental difference between hashing and other binary authentication methods is that hashing is automatic, non-targeted, and cannot be avoided by any internet user.[465] Further, hashing occurs *before* the government has any reason to believe criminal activity is afoot. Every image transmitted via an ECSP is hashed without an individualized suspicion of its sender or recipient. This renders hashing unlike, and significantly more invasive, than other techniques of its kind.

By contrast, individual property is only subject to canine sniffs or spot tests—other forms of binary authentication—*after* the government has an articulable suspicion that a specific person has committed a crime. In fact, the *Place* majority, in articulating that probable cause was not required for a canine sniff, concluded that "the principles of *Terry* and its progeny" allowed the officer to briefly detain luggage to expose it to a canine sniff, "*to investigate the circumstances that aroused his suspicion*."[466] Similarly, the *Jacobsen* Court predicated its acceptance of a warrantless spot test for cocaine on the fact that the agent already had a reasonable suspicion for the test, and that there was a high probability that the suspect possessed contraband.[467] Thus, warrantless canine sniffs and spot tests are legally justified because they are discerning, targeted, and typically do not effect individuals unless they are suspected of a crime.[468] Canine sniffs are employed in response to

---

fees associated with mistakes and how a trained canine costs between $5,000–$25,000).

463 *See* Surden, *supra* note 320, at 1618.

464 Ohm, *supra* note 131, at 39.

465 *See supra* Part I.A.

466 United States v. Place, 462 U.S. 696, 706 (1983) (emphasis added).

467 United States v. Jacobsen, 466 U.S. 109, 122 (1984) ("The field test at issue could disclose only one fact previously unknown to the agent—whether or not a *suspicious white powder* was cocaine." (emphasis added)).

468 *See generally, e.g.*, *Jacobsen*, 466 U.S. 109; *Place*, 462 U.S. 696.

a specific threat, or in certain locations, such as borders or airports.[469] Thus, if an individual wants to avoid a narcotics-sniffing dog, they could plausibly do so. Spot tests are used after a suspect has been identified, a substance has been seized from them, and the government suspects that substance is contraband. Like canine sniffs, spot tests are neither common nor pervasive.

2. Hashing is Less Costly Than Other Binary Authentication Methods

Private ECSPs install hash-value matching software on their own volition.[470] Thus, the government does not spend any money to participate in an evidence gathering dynamic with ECSPs.[471] Since the PROTECT Act requires ECSPs with actual knowledge of child abuse images to disclose these contraband images to law enforcement, matching hash-values are reported directly to the government.[472] Moreover, other types of consumer data are readily available for government acquisition via a § 2703(d) subpoena. The statutory framework regulating the collection and sharing of consumer data is porous, allowing the government to routinely obtain related consumer data, at no cost, and without an onerous showing of suspicion.[473]

Finally, hash-value matching's error rate is practically zero.[474] Therefore, the cost of subsequent litigation due to false hits is non-existent.[475] In sum, hashing software allows law enforcement a cost-free route to "sniff-out" digital contraband sent by any

---

469 *See* Jerierski et al., *supra* note 435, at 112.

470 *Id.*; United States v. Miller, No. 16-47-DLB-CJS, 2017 WL 2705963, at *1 (E.D. Ky. June 23, 2017) (Google has been using its proprietary hashing software since 2008, specifically to assist in the interception of online child abuse images).

471 *See supra* Part I.A.

472 *See supra* Part I.A.2.

473 *See supra* Part I.A.3. Both doctrines rely on the idea that "[a] private search extinguishes an individual's reasonable expectation of privacy in the object searched." *See e.g.*, Adams, *supra* note 186, at 1–2. In both circumstances, courts have held that once frustration of an individual's expectation of privacy occurs by a private actor, the Fourth Amendments does not prohibit governmental use of the now "non-private information." *Id.* at 2.

474 *See supra* Part I.A.

475 *See supra* Part I.A.

individual over the internet, without a particularized suspicion of wrongdoing. Additionally, courts have not scrutinized hashing due to its binary nature—despite the fact it allows for pervasive monitoring that was unthinkable at the time *Place* was decided.[476] Thus, hashing software has caused a rights-shift, eroding the structural privacy right to be free from pervasive government monitoring. This rights-shift has tilted the Fourth Amendment balance toward law enforcement. Under the framework proposed by this Note, hashing is therefore an "exceptional" technology.

C. How Will Hashing Be Treated by the Post-Carpenter Framework?

1. A Fourth Amendment Inquiry will not be Foreclosed Due to Hashing's Binary Nature

The binary search doctrine focuses on the surveillance technique used by law enforcement, as opposed to the information targeted.[477] Thus, applying the binary search doctrine to an exceptional technique runs afoul of *Carpenter*'s test, which specifically addresses the class of information collected.[478] Moreover, *Carpenter* implicitly addressed a frightening possibility of the binary search doctrine: the more tailored an investigative technique is to detecting contraband, the less the public can reasonably expect the law to protect them against government intrusions.[479] This possibility is why the *Carpenter* court chose to aim its analysis at the class of information collected.[480] Since surveillance techniques are becoming even more tailored and efficient, the Court attempted to adjust the resulting Fourth Amendment imbalance by departing from an analysis aimed at the techniques; and instead addressing the information they seek.

---

476 United States v. Place, 462 U.S. 696, 707 (1983) ("[T]he canine sniff is *sui generis.* We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure.").

477 *See id.*

478 *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

479 *See id.* at 2219.

480 *See id.* at 2216–17.

2. A Fourth Amendment Analysis will not be Automatically Foreclosed by an ECSP's Private Search

Carpenter's treatment of the third-party doctrine will guide the Court's treatment of the private search doctrine, a subset of the former. Since hashing is "exceptional," courts should decline to analogize it to pre-digital technologies, such as dog sniffs or spot tests, when assessing whether the private search doctrine forecloses a constitutional inquiry into the government's actions. The *Carpenter* majority endorsed a "poly-analogical" approach to exceptional technologies in lieu of a traditional, REP analysis. Therefore, although an ECSP "searches" user data before law enforcement, in the same way that a wireless carrier views CSLI-evidence before law enforcement, the private intermediary will not necessarily foreclose an inquiry into the constitutionality of law enforcement's warrantless search of hash evidence.

3. The Court Will Apply the *Carpenter* Factors to the Class of Information Sought

Moreover, due to the parallel reasoning underlying the private search and third-party doctrines; the applicability of the private search doctrine to hashing can be neatly analyzed via the three factors posed in *Carpenter*.[481] As a preliminary matter, under *Carpenter*, the Court will tailor these inquiries toward the type of information sought by the technology at issue. With hash-value matching, the information sought is contraband images contained within digital communications.

Like other binary authentication methods, the class of information sought in hashing cases traditionally prompts a reviewing court to adopt an innocence theory of Fourth Amendment rights. Since hashing, by its nature, only reveals contraband, it is tempting for a court to foreclose any further inquiry into its constitutionality and deem such a method outside the amendment's scope. But, investigative techniques are only becoming more tailored. We are heading toward a technological era where Loewy's divining rod will exist, and law enforcement

---

[481] *See Carpenter*, 138 S. Ct. at 2223; *supra* Part I.C.1.

will be able to scan the physical world for evidence of wrongdoing—drawing out only the guilty.

The Orwellian future made possible by technological innovation underscores this Note's proposal to apply a formalist approach to binary authentication cases. That is not to say that most binary authentication methods will violate the Fourth Amendment. Likely, these methods will not constitute a search. However, foreclosing an analysis based the technique's ability to target only the guilty creates a slippery slope, and could lead to future governmental abuse.

Next, courts should recognize hashing's "exceptional" nature when deciding to apply a formalist approach to hashing cases. In earlier binary authentication cases, a presumption of constitutionality in binary search cases was more reasonable because the government already possessed some amount of individualized suspicion before performing the secondary privacy invasion. By contrast, images are routinely hashed without any suspicion at all. Thus, a reviewing court should note hashing's exceptional nature when applying the *Carpenter* factors.

First, contraband contained within digital communications is "deeply revealing" under Justice Robert's test. Even a single image attached to an email may be of a deeply intimate nature. As discussed by the Sixth Circuit in *Warshak*, "[s]ince the advent of email . . . [p]eople are now able to send sensitive and intimate information instantaneously. . . . [L]overs exchange sweet nothings and businessmen swap ambitions plans, all with the click of a mouse. . . ."[482] The *Warshak* Court describes an email account as "an account of its owner's life," access to which would give government agents the ability to peer deeply into one's most intimate secrets. Thus, the deeply revealing information factor cuts in favor of a warrant requirement.

Since the deeply revealing factor highlights the connection between the intimate nature of the data at issue and a Fourth Amendment right over that data, it is helpful to look at the recognized right protecting the content of email communications.

---

[482] United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).

Before the early 2000s, individuals enjoyed a structural right to be free from comprehensive monitoring of their emails contents—which society reasonably expects the government will not engage in. As technology advanced, and such monitoring became possible, circuit courts intervened and expressly held that individuals had Fourth Amendment rights over their email content. Hashing's disclosure of an image that precisely matches an image sent by a user, reveals part of the email's content to the government. Thus, the deeply revealing nature factor cuts in favor of hashing constituting a search.

The second factor highlights the Court's willingness to protect information that possesses "depth, breadth, and comprehensive reach."[483] First, Robert's depth factor is inapplicable to hashing and does not cut in either direction. The *Carpenter* court referred to depth to indicate the precision of an amalgamation of *metadata*. By contrast, hashing reveals *content* data. Hashing is perfectly "precise"—but not in the sense discussed by Justice Roberts.

Moreover, hashing likely does not fulfill the "breadth" factor. Hashing, unlike digital location tracking, does not "store" information on its users. Hashing software either indicates that a user uploaded a matching, contraband, image, and further reviews that image; or fails to find a match and allows the image to metaphorically "flow" past the ISP's bottleneck, to its intended recipient. As for "comprehensive reach," although every *communication* flowing through an ISP is hashed, an ISP does not use hashing software to track its users the way that wireless carriers do via CSLI. Again, because hashing does not "store" information on its users, its reach should not be considered "comprehensive" in the *Carpenter* sense. Thus, the second factor cuts against finding a search.

Finally, the Carpenter majority looked to the "inescapable and automatic nature" of how the information is collected.[484] Compliance with hashing software is an inescapable caveat of using an ECSP, including having an email account. Email is undoubtedly an indispensable part of the information age. Over the

---

483 *Carpenter*, 138 S. Ct. at 2223.

484 *Id.*

last decade, email has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification."[485] Further, hashing is automatic and indiscriminate. One cannot "opt-out" of having their correspondences hashed if they choose to use email services. For these reasons, the "inescapable and automatic nature" factor cuts toward a warrant requirement for hash evidence.

CONCLUSION

To conclude, this Note uses hash-value matching to exemplify how information shared with an ECSP will be treated by the Fourth Amendment in the digital age. It poses a new framework for treating novel technologies and adopts an "equilibrium adjustment" approach to the Fourth Amendment.[486] This framework first asks whether the technology is "exceptional," meaning it disrupts the current balance of power struck by the Fourth Amendment.[487] It proposes looking at whether the technology causes a "rights-shift" to determine if the Fourth Amendment balance has been disrupted; rendering a technology exceptional.[488] Moreover, it adopts Bankston and Soltani's cost centered approach to determining if a rights-shift occurred—which looks at how much less a new technology costs compared to others of its kind.[489]

This Note proposes that exceptional technologies should not be analogized to their conventional predecessors.[490] It analyzes and recommends the *Carpenter* Court's "poly-analogical," holistic approach to exceptional technologies.[491] Finally, this Note assesses whether hashing is an exceptional technology, and how the Courts will treat warrantless hash-value matching after *Carpenter*.[492]

---

485 City of Ontario v. Quon, 560 U.S. 746, 760 (2010).
486 *See supra* Part II.A.
487 *See supra* Part II.A.1.
488 *See supra* Part II.A.2.
489 *See supra* Part II.A.3.
490 *See supra* Part III.B.
491 *See supra* Parts II.B–III.B.
492 *See supra* Parts III.A–III.B.