University of the Pacific Law Review

Volume 53
Issue 1 *SYMPOSIUM—FOR WHOSE BENEFIT PUBLIC CORPORATIONS? PERSPECTIVES ON SHAREHOLDER AND STAKEHOLDER PRIMACY*

Article 16

1-1-2021

Two Models of The Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material

Tyler O'Connell

Two Models of The Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material

*Tyler O'Connell**

TABLE OF CONTENTS

* J.D. Candidate, University of the Pacific, McGeorge School of Law, to be conferred May 2022; B.A. History, California State University, Chico 2014. I am grateful to the editorial board for their attention to detail throughout the publication process. I would also like to thank Distinguished Professor of Law Michael Vitiello for his time and encouragement toward making me a better "sander." Finally, my heart goes out to those victimized by online abuse and my encouragement goes to those seeking to make those crooked places straight.

I. INTRODUCTION

On April 22, 2013, America Online's ("AOL") image detection and filtering process ("IDFP") flagged an email that contained child sexual abuse material ("CSAM").[1] These automated IDFP systems are programs that scan files contained within emails moving across AOL's network for matches to previously scanned and cataloged images of CSAM.[2] As a result of the scan, AOL analysts closed the suspicious email's sender account and submitted a report to the National Council for Missing and Exploited Children ("NCMEC").[3] This congressionally sanctioned non-profit agency spearheads investigations into child abuse and online victimization.[4] The NCMEC opened the email's contents and confirmed it contained illicit material.[5] The NCMEC then relayed the results of its scan to a federal and local law enforcement task force that further investigated, and subsequently charged, Walter Ackerman for distributing CSAM.[6]

These investigations, unfortunately, are all too common for both private tech companies and the NCMEC.[7] With the dawn of the Internet Era in the early 1990s, user proliferation of pornography was among the Internet's first—and among its most common—occurrences.[8] There is national consensus for the legality of pornography depicting consenting adults, yet CSAM also took root online despite Congress' prior illegalization of it in physical mediums.[9] In a case from 1982, the

1. United States v. Ackerman, No. 13–10176–01–EFM, 2014 WL 2968164, at *3 (D. Kan. Jul. 1, 2014); *see also Child Sexual Abuse Material: Overview*, NAT'L CTR. FOR MISSING AND EXPLOITED CHILDREN, https://www.missingkids.org/theissues/csam (last visited Oct. 27, 2020) (on file with the *University of the Pacific Law Review*) ("Outside of the legal system, NCMEC [The National Center for Missing and Exploited Children] chooses to refer to these images as Child Sexual Abuse Material (CSAM) to most accurately reflect what is depicted – the sexual abuse and exploitation of children.").

2. *See Ackerman*, 2014 WL 2968164, at *3 ("AOL's IDFP detected an email sent by 'plains66952@aol.com' to 'zoefeather@riseup.net,' which contained a hash value of previously identified child pornography.").

3. *Id.*

4. *Id.* at *2.

5. *Id.* at *3.

6. *Id.* at *4.

7. *See Technology Has Made It Easier to Harm Kids*, THORN, https://www.thorn.org/child-sexual-exploitation-and-technology/ (last visited Oct. 30, 2020) (on file with the *University of the Pacific Law Review*) (noting over a 15,000% increase in reported files of CSAM to the NCMEC between 2004 and 2019).

8. *See* Charles Apple, *How the Web was Won: Tim Berner's-Lee and the Birth of the World Wide Web*, SPOKESMAN REV. (Oct. 29, 2019), https://www.spokesman.com/stories/2020/jun/22/history-world-wide-web/ (on file with the *University of the Pacific Law Review*) ("[In 1994] [t]he first official White House website launches at whitehouse.gov. Users who type in whitehouse.com get a rude surprise: A porn site has already taken that address.").

9. *See* Protection of Children Against Sexual Exploitation Act of 1977, 92 Stat. 7 (1978) (codified as

United States Supreme Court unanimously held that sexually explicit images depicting minors are not entitled to any constitutional protection on free speech grounds.[10] Yet, Congress took decades to amend child sexual exploitation laws to adapt to the ever-changing landscape of persistent illicit trafficking in CSAM.[11] In combination with these statutory prohibitions, law enforcement and private companies have begun utilizing technological solutions—such as hash value scanning—to combat CSAM's persistent presence online.[12]

Digital surveillance presents several Fourth Amendment issues that seek to balance the needs of effective law enforcement and individual privacy and property rights.[13] Courts have employed various tests to determine what constitutes a digital search for the purposes of the Fourth Amendment.[14] But, as technologies continue to develop at a blistering pace, judges have understandably struggled to apply the 18th century-drafted Constitution with consistency to these changing realities.[15] Courts often vary on when they will shield digital data from unwarranted private-party, law enforcement, or government agency searches.[16] As digital surveillance like hash scanning and facial recognition become more commonplace, courts will need to develop clearer Fourth Amendment tests.[17]

Further complicating this already challenging area of the law is that the predominant view of what the Fourth Amendment protects has evolved over

amended at 18 U.S.C. §§ 2251–52 (2021) ("Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct . . . shall be punished as provided under subsection (e), . . . if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.").

10. New York v. Ferber, 458 U.S. 747, 765 (1982).

11. ADRIENNE L. FERNANDES-ALCANTARA, CONG. RSCH. SERV., RL34050, THE MISSING AND EXPLOITED CHILDREN'S (MEC) PROGRAM: BACKGROUND AND POLICIES 2 (2019).

12. Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38 (2005) ("Hashing is a powerful and pervasive technique used in nearly every examination of seized digital media.").

13. *See id.* at 46 (arguing that the interests of both law enforcement and digital privacy rights are served by utilizing such technological solutions).

14. *See* Jeff Kosseff, *Private Computer Searches and the Fourth Amendment*, J.L. & POL'Y FOR INFO. SOC'Y 187, 190 (2018) (outlining court's trends toward utilizing the "agent-or-instrument" test when a private entity performs the digital data collection and later provides the content to the government); *see also infra* Parts III–VI (discussing the various search doctrines including third-party doctrine, plain view, and the impacts technology has had on these approaches).

15. Alain Leibman, *Computer Search and Seizure Under the Fourth Amendment: The Dilemma of Applying Old-Age Principles to New-Age Technology*, U.S. L. WEEK (Mar. 14, 2011), https://news.bloomberglaw.com/white-collar-and-criminal-law/computer-search-and-seizure-under-the-fourth-amendment-the-dilemma-of-applying-old-age-principles-to-new-age-technology (on file with the *University of the Pacific Law Review*).

16. *See generally* Kosseff, *supra* note 14 (outlining the difficulties in applying the third-party doctrine to private versus government searches and discussing the varying circuit court approaches to applying subjective versus objective factors in determining whether a search has occurred).

17. *See infra* Part V (arguing that common law analogues to metadata hash scanning exist which similarly establish probable cause, such as; dog sniffs, plain view, and pat downs).

time.[18] Originalists conceive of the Fourth Amendment as concerning the rights of the individual over their *property*.[19] This practical and textual interpretation is based in the amendment's prohibitory language barring unreasonable searches of citizens' "persons, houses, papers, and effects."[20] One scholar described the Amendment as "textually limited to . . . places or things."[21] Parallel to this interpretation, living constitutionalists view the Supreme Court's *Katz* decision as the lodestar of any Fourth Amendment analysis—which they interpret as prioritizing *privacy* over property rights.[22] While both views seek to capture the spirit and text of the Fourth Amendment, the Court has embraced a middle path—a property-plus approach.[23]

This Comment argues that digital surveillance technologies like hashing strike a constitutional balance between the property and privacy rationales.[24] Hash scans only minimally intrude upon individual personal property rights as these scans reveal only metadata and no actual content.[25] At the same time, hash value scans maintain the digital privacy interests of users by limiting metadata access to automated algorithms that do not reveal "the privacies of life."[26] Yet, along with this privacy rationale comes other jurisprudential baggage that complicates private companies ability to scan for illicit content.[27]

---

18. *See* Michael Vitiello, Katz v. United States: *Back to the Future*, 52 U. RICH. L. REV. 425, 425 (2018) ("*Katz*, as originally conceived, holds promise for the future. Its core holding, not limited by property-trespass concepts, provides a framework for the Court to vitalize privacy protections, even in an era of increasingly invasive technologies.").

19. *See* United States v. Jones, 565 U.S. 400, 405 (2012) ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures;' the phrase 'in their persons, houses, papers, and effects' would have been superfluous."); *compare* United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that a tracking device which recorded *movements on a public roadway* was not a search, as the surveillance took place in "plain view"), *with* United States v. Karo, 468 U.S. 705, 716 (1984) (holding that a similar tracking device to that used in Knotts *which recorded activity inside the suspect's home* was a search because it was "[i]ndiscriminate monitoring of property that has been withdrawn from public view").

20. U.S. CONST. amend. IV.

21. ORIN S. KERR, THE DIGITAL FOURTH AMENDMENT: IMPLEMENTING CARPENTER (Oxford Univ. Press, forthcoming) (manuscript at 6).

22. *See, e.g.*, Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, 129 (2018) ("*Katz* focuses on whether an individual intended to keep information private and whether information had been previously disclosed.").

23. *See* KERR, *supra* note 21, manuscript at 6 ("[T]he Supreme Court's application of *Katz* has closely traced the Fourth Amendment's focus on places and things. That location focus is the heart of what the Fourth Amendment protects.").

24. *Infra* Parts III–VI.

25. *What Is a Hash? And How Does It Work?*, SENTINELONE BLOG (May 22, 2019), https://www.sentinelone.com/blog/what-is-hash-how-does-it-work/ (on file with the *University of the Pacific Law Review*).

26. Riley v. California, 573 U.S. 373, 403 (2014); Salgado, *supra* note 12, at 39.

27. *See infra* Section IV.C (discussing the technical distinctions under the expansion-of-the-search doctrine that can be dispositive for a court's determination of whether a hash scan has violated a person's Fourth Amendment rights).

The most troublesome outgrowth from the Supreme Court's privacy cases is the third-party doctrine, which provides that individuals have no expectation of privacy in information they voluntarily give to third parties.[28] This rule finds itself clinging to life in the Internet Era, and current Justices on the Supreme Court appear willing to remove it from life support.[29] Admittedly, technologies like facial recognition fall squarely on the privacy side of the Fourth Amendment line.[30] Such invasive technologies require that cogent Fourth Amendment interpretation preserve both the privacy and property rights interpretations to effectively protect Americans' online data.[31] Yet, technologies like hashing satisfy the Fourth Amendment restrictions of either rationale and allow law enforcement to effectively investigate and prosecute CSAM.[32] Courts will need to modify or abandon some search law doctrines in the face of these challenges—especially the third-party doctrine.[33] Further, as states continue protecting individuals' online data as quasi-property, courts will need a new test for determining if hash scans comport with this post-physical interpretation.[34]

The following section outlines the current state of federal CSAM prohibitions and current technological methods allowing private companies and law enforcement to investigate illicit material online.[35] Part III describes the privacy model of the Fourth Amendment and the effect that rationale has had on hash scanning—stemming from the *Katz* decision.[36] Part IV highlights Internet Era problems with the privacy model's thorny offshoot, the third-party doctrine.[37] Part V discusses common law analogues to hash scanning that respect privacy and property rights while also allowing for investigators to effectively prosecute CSAM traffickers.[38] Part VI briefly discusses the current flux in the Supreme Court

28. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

29. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2235, 2246 (2018) (Thomas, J., dissenting) ("This case should not turn on 'whether' a search occurred. It should turn, instead, on *whose* property was searched . . . the *Katz* test is a failed experiment"); Vitiello, *supra* note 18, at 425 ("Faced with technology that has eroded privacy expectations, the Court may be ready to reexamine its post-*Katz* case law.").

30. *Infra* Section II.D.

31. *Infra* Section II.D.

32. *Infra* Parts III–V.

33. *See Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting) (internal quotations omitted) ("In the years since its adoption, countless scholars, too, have come to conclude that the third-party doctrine is not only wrong, but horribly wrong."); *infra* Parts III–VI.

34. *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (giving Californians' rights over the use, retention, transfer, and deletion of their online data); *see also* 740 ILL. COMP. STAT. 14 §§ 5–20 (West 2021) (providing Illinois residents with similar rights over the use, transfer, and deletion of their online biometric data—including availability of civil damages for misappropriation).

35. *Infra* Part II.

36. *Infra* Part III.

37. *Infra* Part IV.

38. *Infra* Part V.

on whether *Katz*, property law rules, or some combination will govern digital searches in the near future.[39] Part VII concludes that strenuous constitutional protection for Americans' data, under either model of the Fourth Amendment, need not impede successful CSAM prosecutions.[40]

II. MODERN LEGAL PROHIBITIONS AND METHODS FOR INVESTIGATING CSAM

When Congress first prohibited CSAM, traffickers were limited to sharing this material in only physical form, drastically reducing their ability to produce and share it.[41] Early Senate Judiciary Committee reports highlighted the legislation's physical focus—which prohibited CSAM in "still photographs, slides, playing cards, and video cassettes"—among other tangible mediums.[42] Aggressive legislation, judicial enforcement, and law enforcement investigations led to a sharp decline in reported cases of trafficked CSAM in the mid-to-late 1990s.[43] One prosecutor described the laws prohibiting CSAM as some of the "fiercest criminal laws" on record.[44]

Yet, especially since 2000, the Internet has opened a veritable pandora's box, allowing traffickers to almost effortlessly share CSAM online.[45] New technologies such as email, social media, cloud-based storage, and peer-to-peer networking have enabled traffickers to more easily produce and widely share this horrific content.[46] Furthermore, such a sea change has dramatically altered the landscape for investigating and prosecuting individuals who abuse children.[47] Worse still is that, once a trafficker shares explicit images of a child online, the impacts on that victim never truly dissipate.[48] Unsurprisingly, this "victimization lasts forever"

39. *Infra* Part VI.

40. *Infra* Part VII.

41. *See* S. REP. NO. 95–438, at 5–6 (1977) ("[O]ne researcher . . . has documented the existence of over 260 different magazines which depict children engaging in sexually explicit conduct.").

42. *Id.* at 6.

43. *Technology Has Made It Easier to Harm Kids*, *supra* note 7; *see* FERNANDES-ALCANTARA, *supra* note 11, at 2 (outlining the development of the dramatically increased social, statutory, and law enforcement attention to the proliferation of CSAM up to the present day).

44. Gabriel J.X. Dance & Michael H. Keller, *How Laws Against Child Sexual Abuse Imagery Can Make It Harder to Detect*, N.Y. TIMES (Nov. 12, 2019), https://www.nytimes.com/2019/11/12/us/online-child-sex-abuse.html (on file with the *University of the Pacific Law Review*).

45. *Microsoft Expands PhotoDNA to Fight Child Abuse Imagery*, THORN, https://www.thorn.org/blog/microsoft-expands-photodna-to-fight-child-abuse-imagery/ (last visited June 3, 2021) [hereinafter *Microsoft Expands PhotoDNA]* (on file with the *University of the Pacific Law Review*).

46. Sarah Chang & Keith Becker, *Child Pornography Conspiracies in the Digital Age: A Primer*, 62 U.S. ATT'Y'S BULL. 75, 75 (2014).

47. *Id.*

48. Audrey Rogers, *Child Pornography's Forgotten Victims*, 28 PACE L. REV. 847, 853 (2008) (noting that images of CSAM "can resurface at any time" and this recirculation process has only increased since the advent of the Internet).

online, since neither platforms nor investigators can ever truly erase this content from the Internet's darkest corners.[49]

Section A surveys the current state of federal laws prohibiting persons from producing, sharing, or receiving CSAM.[50] Section B introduces the congressionally mandated national clearinghouse for assisting with the investigation of child sexual abuse cases—the NCMEC.[51] Section C provides a description of technological investigation methods—which private companies primarily conduct given their exclusive access—framing investigator's ability to investigate, confirm, and catalog CSAM.[52] Finally, section D discusses new technology—facial recognition databases—that will further shift the landscape on which these investigations take place.[53]

A. United States Federal Child Pornography Laws

The United States Department of Justice Child Exploitation and Obscenity Section—along with many other multi-agency task forces—enforces federal CSAM laws.[54] Images of CSAM are unprotected speech; therefore, federal and state agencies may vigorously prosecute traffickers of this contraband.[55] These statutes prohibit virtually any activity involving persons' production, possession, distribution, or receipt of CSAM—with harsh prison terms.[56]

B. The National Council for Missing and Exploited Children

In 1984, Congress passed the Missing Children's Assistance Act.[57] This Act directed the United States Department of Justice ("DOJ") to establish a "national resource center to respond to cases of missing and exploited children."[58] Child advocates founded the NCMEC in coordination with the DOJ to fulfill this

---

49. *Id.*

50. *Infra* Section II.A.

51. *Infra* Section II.B.

52. *Infra* Section II.C.

53. *Infra* Section II.D.

54. *Child Exploitation and Obscenity Section*, U.S. DEPT. OF JUST., (2020) https://www.justice.gov/criminal-ceos (last visited Sept. 8, 2021) (on file with the *University of the Pacific Law Review*); *see also* 18 U.S.C. §§ 2251–60 (West 2021) (outlining the production, possession, distribution, and receipt of child pornography as illicit and punishable by up to 30 years in prison).

55. *See* New York v. Ferber, 458 U.S. 747, 765 (1982) (holding that a New York state statute, similar to 18 U.S.C. § 2251, "sufficiently describes a category of material the production and distribution of which is not entitled to First Amendment protection"); *see also* United States v. Henry, 827 F.3d 16, 24–25 (1st Cir. 2016) (holding that the lower court's failure to read in a "mistake of age" defense into § 2251 did not violate the First Amendment); *Citizen's Guide to U.S. Federal Law on Child Pornography*, U.S. DEPT. OF JUST., https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography (updated May 28, 2020) [hereinafter *Citizen's Guide*] (on file with the *University of the Pacific Law Review*).

56. *Citizen's Guide*, *supra* note 55.

57. FERNANDES-ALCANTARA, *supra* note 11, at *Summary*.

58. *Id.*

congressional mandate.[59] The NCMEC created the CyberTipline in 1998 to provide "an online mechanism for members of the public and electronic service providers ("ESPs") to report incidents of suspected child sexual exploitation."[60] Congress has vested considerable authority in the NCMEC to work collaboratively with federal, state, and local law enforcement to achieve its missions.[61]

The NCMEC has seen astronomical increases in the number of CSAM reports it receives from private tech companies since 2000.[62] In the decade of the 2000s, investigators saw nearly a five-fold increase in the number of arrests for production of child abuse imagery.[63] Since 2004, the NCMEC has seen over a 15,000 percent increase in the number of reported files containing CSAM.[64] The NCMEC has reported a further 28% increase in total reports received from private companies from 2019 to 2020.[65] These dramatic reporting and enforcement increases are based in part on ease of access for purveyors and viewers alike.[66] Yet, these increases are also lagging indicators of third-party tech company platforms' increasing proactivity in cataloging, scanning, and isolating this harmful content.[67]

C. Hash Value Tagging CSAM

Hashing is the primary means by which platforms mitigate users' proliferation of this criminal material on their platforms.[68] At its most basic level, a hash is a

59. *Our Beginnings*, NAT'L CTR. FOR MISSING AND EXPLOITED CHILDREN, https://www.missingkids.org/footer/about/history (last visited Oct. 27, 2020) (on file with the *University of the Pacific Law Review*).

60. *Id.*

61. FERNANDES-ALCANTARA, *supra* note 11, at 8 ("In addition to funding through the [Missing and Exploited Children's] MEC program, NCMEC is also funded through private contributions, other DOJ grants, and the United States Secret Service in the Department of Homeland Security (DHS). Pursuant to the Violent Crime Control and Law Enforcement Act of 1994 (P.L. 103–322), Congress has mandated that the United States Secret Service [("USSS")] provide forensic and technical assistance to NCMEC and federal, state, and local law enforcement agencies in matters involving missing and exploited children. In recent years, funding provided by the USSS has been transferred to OJP to be provided directly to NCMEC.").

62. *Technology Has Made It Easier to Harm Kids*, *supra* note 7.

63. JANIS WOLAK ET AL., UNIV. OF N.H. CRIMES AGAINST CHILDREN RES. CTR., TRENDS IN ARRESTS FOR CHILD PORNOGRAPHY PRODUCTION: THE THIRD NATIONAL JUVENILE ONLINE VICTIMIZATION STUDY, 1 (2012).

64. *Technology Has Made It Easier to Harm Kids*, *supra* note 7 (noting that in 2004 there were 450,000 files reported to the NCMEC, compared to 70 million in 2019).

65. *Why an Increase in Reports of CSAM is Actually a Good Thing*, THORN, https://www.thorn.org/blog/why-an-increase-in-reports-of-csam-is-actually-a-good-thing/ (last visited Oct. 30, 2020) (on file with the *University of the Pacific Law Review*).

66. *See id.* ("[I]f there's an upload button on a platform, it will be used to host child sexual abuse material.").

67. *Id.*

68. *How Safer's Detection Technology Stops the Spread of CSAM*, THORN (Aug. 13, 2020), https://www.thorn.org/blog/how-safers-detection-technology-stops-the-spread-of-csam/ [hereinafter *Safer's Detection Technology*] (on file with the *University of the Pacific Law Review*).

binary, digital code derived from a source file.[69] Like a human "fingerprint," hashing "can be used to identify a file without having to actually look" at the file itself—like a crime scene forensic analyst finding a criminal's fingerprint on an available surface and then cross-referencing that print to a known database for matching.[70] Hash tables visually represent the values as a long string of seemingly random letters and numbers.[71] When analysts create hash tables, they can identify when a previously hashed file, or its duplicate, is present or moves across a network—such as in email.[72] Common algorithms generate sequences "so distinct that the chance that any two data sets are given the same hash value is less than one in one billion."[73] Platforms use hashes for a number of purposes distinct from locating and isolating CSAM, such as tracking and eliminating malware.[74] More recently, platforms have realized the efficiency of consistently using hashes for cataloging, identifying, and reporting user proliferation, distribution, and receipt of CSAM.[75]

Importantly, when analysts generate hash values, their programs scan and scrub all content of the file for which it creates a hash.[76] Meaning, companies do not view *actual content* of the file when scanning its hash value.[77] This prevents platforms from perusing users' content at will.[78] Only an automated scan of the network or database and subsequent identification of a hash value match to known CSAM justifies an analyst opening a file.[79] To effectively locate future matches, platforms retain extensive logs of previously identified CSAM hashes—without their content—for cross-reference to isolate and report matches.[80]

Finally, as more companies become aware of the problem, they have begun sharing their catalogs of hashes with other private companies, the NCMEC, and

---

69. *What is a Hash?*, *supra* note 25.

70. *Safer's Detection Technology*, *supra* note 68.

71. *See What Is a Hash?*, *supra* note 25 (providing an example of a hash with its core components as: (1) the algorithm—the means of creating the assigned alphanumerical code—such as, SHA-1, SHA-2 256 or MD5; (2) the coded hash value, such as, "CAF110E4AEBE1FE7ACEF6DA946A2BAC9D51EDCD47A987E311599 C7C1C92E3ABD"; and (3) the file's path—meaning location on the computer, drive, or network—such as, "C:/Users/sphil/Desktop/ship.jpg").

72. *See What Is a Hash?*, *supra* note 25 (analogizing hash tables to human "fingerprints," where analysts can then cross-reference for comparison, and subsequent identification, of CSAM).

73. *An Introduction to Hashing: A Powerful Tool to Detect Child Sexual Abuse Imagery Online*, THORN (Apr. 12, 2016), https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery/ (on file with the *University of the Pacific Law Review*).

74. *See What Is a Hash?*, *supra* note 25 (describing malware as files that contain malicious code which will harm computer systems).

75. *An Introduction to Hashing*, *supra* note 72.

76. *What Is a Hash?*, *supra* note 25.

77. *Id.*

78. *Id.*

79. *Id.*

80. *See, e.g.*, *Microsoft Expands PhotoDNA*, *supra* note 45 (citing PhotoDNA as just one platform that has assisted in "photo sharing" with other companies in order to execute "the removal of millions of illegal photos across the web").

law enforcement.[81] This collaboration expedites the accuracy and efficiency of private-party detection, reporting, and cataloging.[82] Hashing technology, while complex, is in fact a relatively simple method for tech companies to monitor illicit digital content without actually exposing its users' data.[83]

D. Clearview AI & Facial Recognition Technology

Over the horizon, facial recognition technology is promising for even further expanding law enforcement's ability to protect victims of CSAM.[84] One company—Clearview AI—adopted facial recognition as its focus early on and has become a leader in the industry despite, admittedly, violating platforms' terms of service agreements.[85]

Many officers in law enforcement find the size and scale of Clearview AI's repository for matching digital images of individuals online most impressive.[86] Clearview AI operates by allowing subscribers—typically law enforcement officers—to upload "probe images" of a victim or suspect of a crime.[87] The program then uses its facial recognition technology and scans its database of over three billion images across millions of websites to retrieve all images matching the probe image.[88] The program then links investigators to any known web profiles—such as Facebook, LinkedIn, or other sites—of the identified person.[89]

---

81. *What Is a Hash?*, *supra* note 25.

82. *See Microsoft Expands PhotoDNA*, *supra* note 45 (citing "over 70 companies" currently utilizing PhotoDNA's algorithms to detect and remove CSAM).

83. *See* Salgado, *supra* note 12, at 38 ("The concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data.").

84. *See, e.g.*, Kashmir Hill, *The Facial-Recognition App Clearview Sees a Spike in Use After Capitol Attack*, N.Y. TIMES (Jan. 9, 2021), https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html (on file with the *University of the Pacific Law Review*) (reporting that following the politically motivated disruption of Congressional functions in the halls of Congress, police "are using Clearview to try to identify rioters and are sending the potential matches to the F.B.I.'s Joint Terrorism Task Force . . . [making] one potential match within their first hour of searching").

85. Kashmir Hill, *The Secret Company That Might End Privacy as We Know It*, N.Y. TIMES (updated Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [hereinafter Hill, *The Secret Company*] (on file with the *University of the Pacific Law Review*).

86. *See* Hill, *The Secret Company*, *supra* note 85 ("The system—whose backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites—goes far beyond anything ever constructed by the United States government or Silicon Valley giants.").

87. *See* Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App is Identifying Child Victims of Abuse*, N.Y. TIMES (updated Feb. 10, 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html [hereinafter Hill & Dance, *Clearview's Facial Recognition App*] (on file with the *University of the Pacific Law Review*) (describing these probe images as the starting point for any facial recognition search and the template upon which the software bases its search).

88. Hill, *The Secret Company*, *supra* note 85.

89. Hill & Dance, *Clearview's Facial Recognition App*, *supra* note 87.

Over 600 agencies used Clearview AI's search engine during 2020, including federal agencies such as the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security.[90] Investigators vigorously endorse the effectiveness of this technology, as it allows them to quickly and efficiently identify the names and locations of many victims of CSAM.[91] One officer described Clearview AI's capabilities in the hands of law enforcement as "the biggest breakthrough in the last decade" for investigating CSAM crimes.[92]

Yet, critics are less sanguine about law enforcement's desires for widespread implementation of Clearview AI's software.[93] One critic has argued, "exchang[ing] freedom and privacy for some early anecdotal evidence that it might help some people is wholly insufficient to trade away our civil liberties."[94] Another opponent said Clearview AI's tool "could end your ability to walk down the street anonymously," and noted "hundreds of law enforcement agencies" already use it.[95] New Jersey, New York, Virginia, Illinois, and Washington have all taken steps to ban law enforcement's use of such technology.[96] Even Silicon Valley companies—Facebook, LinkedIn, Twitter, Venmo, and YouTube—have issued cease-and-desist letters to Clearview AI, insisting that the company cease scanning user images on their websites.[97] Certainly, Clearview AI's application involves legal and ethical challenges that extend beyond CSAM investigations.[98] Fortunately, the challenges agencies investigating CSAM face may yet be resolved without resorting to such invasive technologies like facial recognition dragnets.[99]

---

90. Rebecca Heilweil, *The World's Scariest Facial Recognition Company, Explained*, VOX (updated May 8, 2020), https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement (on file with the *University of the Pacific Law Review*).

91. Hill & Dance, *Clearview's Facial Recognition App*, *supra* note 87.

92. *Id.*

93. *See id.* (listing both several private companies and individual states which have opposed Clearview's use by tech companies and law enforcement).

94. *Id.*

95. Hill, *The Secret Company*, *supra* note 85.

96. Hill & Dance, *Clearview's Facial Recognition App*, *supra* note 87; *see, e.g.*, 740 ILL. COMP. STAT. 14 §§ 5–20 (West 2021) (discussing Illinois' rigorous Biometric Information Privacy Act which prohibits private companies from sharing "biometric identifiers or biometric information" such as "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" without an express, written release).

97. *See* Hill & Dance, *Clearview's Facial Recognition App*, *supra* note 87 (explaining one tech company CEO's aversion to using facial recognition technologies on his platform's users given "ethical reasons" further noting that "[w]e thought it was too controversial of a feature because it was too easy to use that functionality for abuse, [a]nd also it's just a legal nightmare.").

98. Heilweil, *supra* note 90 (citing numerous civil liberties concerns with such effective, easy-to-use facial recognition technology, including, abuse by rogue law enforcement agents, potential stalking concerns, and use by foreign governments).

99. *See infra* Subsection IV.C.2 (arguing that hash value scanning is a far less invasive method for accomplishing the same legitimate law enforcement goals).

III. THE PRIVACY MODEL OF THE FOURTH AMENDMENT

The judiciary's Fourth Amendment jurisprudence has changed over time—especially in the Internet Era—creating considerable uncertainty.[100] One scholar described the ambiguity as "trying to put together a jigsaw puzzle with several incorrect pieces: no matter [what courts do] a few pieces won't fit."[101] In 1967, the Court sought to shed some light on how best to approach the Fourth Amendment in the modern, technological era.[102] The Supreme Court's "watershed" decision in *Katz v. United States* dramatically altered the judiciary's approach to search law analysis under the Fourth Amendment.[103] To many scholars, *Katz* spawned the privacy rights approach to Fourth Amendment interpretation—now that "the Fourth Amendment protects people, not places" or things.[104] Some scholars continue to describe the case as one where the Court "abandoned the importance of trespass law and reframed the debate in terms of expectations of privacy."[105] This conception of *Katz* certainly finds footing in the facts of the case and the text of the opinion.[106] But the Court frequently reiterates the importance of property law concepts in many areas of its Fourth Amendment jurisprudence.[107]

Section A discusses the Supreme Court's foundational privacy rights case and its corollaries that created the third-party doctrine.[108] Section B examines the curious decision in *Riley v. California*, where the Court seemingly created a digital right to privacy largely out of whole cloth.[109] Section C outlines what a privacy

100. Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 (1985) ("Thus it is apparent that not only do the police not understand [F]ourth [A]mendment law, but that even the courts, after briefing, argument, and calm reflection, cannot agree as to what police behavior is appropriate in a particular case.").

101. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004) [hereinafter Kerr, *Constitutional Myths*] (describing Fourth Amendment law as "unruly" and with "few agreed-upon principles").

102. *See* Katz v. United States, 389 U.S. 347, 350–53 (1967) (balancing what the Court saw as complimentary property and privacy interests at play in the text of the Fourth Amendment).

103. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974).

104. *Katz v. United States*, 389 U.S. at 347.

105. Vitiello, *supra* note 18, at 425.

106. *See Katz v. United States*, 389 U.S. at 351 (rebutting briefs from both sides claiming that monitored oral statements recorded from a device attached to a telephone booth implicated a "constitutionally protected area," as this formulation "deflects attention from the problem presented by this case").

107. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 129 (1990) (emphasis added) (deciding the validity of standing to object to a police search on whether or not the defendant had claimed "*a property [o]r possessory interest*" in the thing searched); Kyllo v. United States, 533 U.S. 27, 34 (2001) (internal quotations omitted) (holding that when police use sense-enhancing technology to obtain "information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area" a search has occurred); United States v. Karo, 468 U.S. 705, 712 (1984) (citing United States v. Jacobsen 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when 'there is some meaningful interference with an individual's possessory interests in that property.'").

108. *Infra* Section III.A.

109. *Infra* Section III.B.

rights model of the Fourth Amendment would mean for governmental and private-party investigation of CSAM cases.[110]

A. Katz v. United States *and Its Corollaries*

In *Katz*, the Supreme Court "changed the emphasis" of Fourth Amendment protection from places and things to "interferences with individual expectations of privacy."[111] This case gave rise to the parallel view in addition to the narrower property approach.[112] *Katz* expanded the inquiry "from a focus on the nature of the object to the nature of the possessor's expectation of privacy."[113]

The federal government convicted Katz of violating illicit wagering statutes, relying on evidence of incriminating statements he made on a telephone call from a public phone booth.[114] To obtain the statements, the FBI had attached an electronic recording device to the outside of the public telephone booth that Katz had used to conduct the transactions.[115] The constitutional issue arose out of the FBI listening in on a private conversation with an "uninvited ear."[116] While sidestepping the property-law-based, "constitutionally protected area" approach, the Court sought to cleave the constitutional baby in two.[117] In charting a middle path, the Court also seemed to remind itself that it could not translate the Fourth Amendment "into a general constitutional right to privacy."[118]

Ultimately, Justice Harlan's concurrence in *Katz* became the Court's most utilized test for determining what constitutes a search for purposes of the Fourth Amendment.[119] Justice Harlan's test delineated two distinct requirements, "first that a person have exhibited an actual (subjective) expectation of privacy."[120] And second, "that the expectation be one that society is prepared to recognize as [objectively] 'reasonable.'"[121]

Katz modified courts' search law analysis, expanding protections beyond the formalistic "constitutionally protected areas" of property law and acknowledging the privacy rights implicit in the Fourth Amendment's text.[122] Yet, property law

110. *Infra* Section III.C.

111. Abraham Bell & Gideon Parchomovsky, *The Privacy Interest in Property*, 167 U. PA. L. REV. 869, 886 (2019).

112. *Id.* at 887.

113. *Id.*

114. Katz v. United States, 389 U.S. 347, 348 (1967).

115. *Id.*

116. *Id.* at 352.

117. *See id.* at 350 ("We decline to adopt this formulation of the issues.").

118. *Id.*

119. JOSHUA DRESSLER ET AL., CRIMINAL PROCEDURE: INVESTIGATING CRIME 98 (West Acad. Pub. 7th ed. 2020).

120. *Katz v. United States*, 389 U.S. at 361 (Harlan, J., concurring).

121. *Id.*

122. *See id.* at 351–53 (majority opinion) (emphasis added) (acknowledging that—while there was "no physical penetration" which would easily implicate the Fourth Amendment under *Olmstead v. United States*—

concepts remained at the root of what the Fourth Amendment protects.[123] Further, one scholar has argued that *Katz* is "better understood as a shift of degree from common law rules to the looser property-based approach that currently governs."[124] Lawmakers and courts have incorporated the privacy-based approach into all manner of statutes and Fourth Amendment search analysis.[125] Nevertheless, property law concepts still remain relevant in the arena of digital surveillance.[126]

Subsection 1 reviews the Supreme Court's early *Katz* corollary case dealing with personal records *in physical form* after a person turns them over to a third party's management and control.[127] Subsection 2 describes an early technology search case dealing with an archaic form of metadata where the Court marshalled the third-party doctrine to undermine property rights.[128]

1. United States v. Miller*: Paper Records*

As scholars have noted, the "third-party doctrine largely traces its roots to *Miller*."[129] The Bureau of Alcohol Tobacco and Firearms was investigating the suspect in *Miller* for conspiring to defraud the U.S. of tax revenues on large shipments of whiskey.[130] Hoping to acquire the evidence needed for conviction, prosecutors subpoenaed Miller's bank for records of fraud.[131] In affirming the trial court's ruling denying Fourth Amendment protection, the Court implied a lack of property or privacy interest in documents Miller gave to a third party.[132] On the property score, Miller could "assert neither ownership nor possession" of the records as they had become "the business record of the banks."[133] According to the Court, Miller's relinquishment of control diminished his expectation of privacy

the government's "recording of the petitioner's words *violated the privacy upon which he justifiably relied* while using the telephone booth . . . and thus constituted a search and seizure").

123. *See* Kerr, *Constitutional Myths*, *supra* note 101, at 815–16 ("[T]he mainstream academic understanding has often overlooked the continuing influence of property concepts because it has tended to misconstrue cases that rejected strict common law property rules as Fourth Amendment guides.").

124. *Id.* at 816.

125. *See* Bell & Parchomovsky, *supra* note 111, at 884 (describing the "mushrooming of privacy rights . . . in many areas of the law" such as in tort and statutes including "such varied topics as medical information, consumer information, government surveillance, bank records, and searches of students at school").

126. *See* Kerr, *Constitutional Myths*, *supra* note 101, at 822 (describing *Katz* as "a Rorschach test" where either interpretation is feasible based on the language in the opinion, but endorsing the "loose property-based approach" as the most workable analytical framework).

127. *Infra* Subsection III.A.1.

128. *Infra* Subsection III.A.2.

129. DRESSLER, *supra* note 119, at 159.

130. United States v. Miller, 425 U.S. 435, 436 (1976).

131. *Id.*

132. *See id.* at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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 party will not be betrayed.").

133. *Id.* at 440.

because the statements "were exposed to [bank] employees in the ordinary course of business."[134]

2. Smith v. Maryland*: Pre-Internet Metadata*

Smith was the Court's first metadata case, before the term metadata even existed.[135] In *Smith*, police were investigating a robbery that had taken place in early March 1976.[136] The victim later complained that she was receiving threatening and obscene phone calls from a man claiming to be the man who had robbed her.[137] Police suspected Smith to be the man responsible, but no probable cause existed for a warrant.[138] In response, police requested the phone company install a pen register at the telephone company's office that recorded all phone numbers dialed from Smith's house.[139] Importantly, the device recorded only the numbers dialed—not any conversations.[140] Using the pen register, police confirmed that Smith had indeed placed the phone calls to the victim.[141] In turn, this confirmation provided police the basis for a warrant to search his home—resulting in his conviction for the robbery.[142]

The Court noted this "pen register differ[ed] significantly from the listening device employed in *Katz*."[143] The crux of the Court's ruling to deny Fourth Amendment protection was the fact that such a device did not monitor "the contents of communications."[144] Further, utilizing the language of *Katz*, the Court also noted that most people have a reasonable expectation that phone companies routinely monitor such metadata.[145] The Court also took note of the third-party rule, where "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[146] Ultimately, the Court viewed Smith's use of the telephone company's lines to implicate no property right of his own, nor any reasonable expectation of privacy.[147]

---

134. *Id.* at 442.

135. *See generally* Smith v. Maryland, 442 U.S. 735 (1979) (describing the case wholly in terms of expectations of privacy and never using the word data or metadata); *see also Metadata: defined*, MERRIAM-WEBSTER, https://www.merriamwebster.com/dictionary/metadata?utm_campaign=sd&utm_medium=serp&utm_source=jsonld (last visited Mar. 13, 2021) (on file with the *University of the Pacific Law Review*) (listing "[t]he first known use of metadata" in 1983).

136. *Smith v. Maryland*, 442 U.S. at 737.

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.*

142. *Smith v. Maryland*, 442 U.S. at 737.

143. *Id.* at 741.

144. *Id.*

145. *Id.* at 742.

146. *Id.* at 743–44.

147. *Id.* at 745–46.

B. Riley v. California*: An Individual Digital Privacy Right?*

Riley represents the Court's first foray into analyzing government searches of mass storage digital devices that are now firmly in the grasp of nearly every American's palm.[148] The opinion launched a new line of Fourth Amendment case law aimed at protecting the privacy of individuals' digital content.[149] Implicit in the opinion was the presence of the petitioner's property interest over the content that the police searched.[150] However, the Court spilled most of its ink addressing the privacy interests involved in such searches.[151]

Police arrested Riley for possessing illegal firearms and searched him, which led the arresting officer to discover Riley's cell phone and other incriminating evidence.[152] The officer opened the phone and examined its recent text message history—"looking for evidence"—and found incriminating photos, videos, and text.[153] The Court spent much time distinguishing such data, "differ[ing] in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[154] The Court weighed several factors such as the immense storage capacity, element of pervasiveness into American life, and the intimacy of the content on such devices.[155] But the opinion only briefly mentioned any "expectations of privacy," to that point a central feature of the Court's privacy-based approach.[156] On its facts, the Court seemed to limit *Riley* to similar factual scenarios: police search a person with a device containing digital evidence, physically on that person.[157]

C. What A Privacy Model of the Fourth Amendment Means for CSAM Investigations

Riley hinted at, but left unaddressed, the problem of third-party managed digital data such as information contained in a cloud storage, online database, or

148. *See* Riley v. California, 573 U.S. 373, 395 (2014) (citing statistics indicating that "more than 90% of American adults" own and keep cell phones on their persons regularly).

149. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (seeking to protect "the privacies of life" against governmental intrusion).

150. *See Riley v. California*, 573 U.S. at 386 (distinguishing the digital content on a flip phone from the content of a physical container, the latter of which an arresting officer may search incident to arrest, as the former lacks the presence of a potential threat to the officer).

151. *See id.* at 386 ("90% of American adults" own cell phones and that these devices often maintain "a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

152. *Id.* at 378–79.

153. *Id.*

154. *See id.* at 393 ("[T]oday many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.").

155. *Id.* at 393–94.

156. *See Riley v. California*, 573 U.S. at 378–81 (listing policy factors in favor of suppression of the illegally obtained digital evidence in place of a formal analytical framework as outlined by *Katz*).

157. *Id.* at 386.

cell network.[158] But the implications for CSAM investigations are significant.[159] Specifically, whether a hash scan invades a person's reasonable expectations of privacy is an issue the Supreme Court has not considered.[160] Reflecting these legal trends and consumer preferences, many lesser known platforms already utilize full end-to-end encryption.[161] Moreover, the major platforms are also considering moving to full encryption—and some already have.[162]

Full end-to-end encryption would prevent platforms from scanning or opening any private-party hashes or content.[163] The continuation of these trends will inevitably undermine the capacity of the NCMEC and law enforcement to effectively investigate CSAM.[164] Furthermore, state legislatures have already begun shielding individuals from private company misappropriations of their biometric data without individuals' consent.[165] In the Internet Era, there is nothing in the third-party rule that would impede Orwellian facial recognition dragnets from companies like Clearview AI.[166] And third-party hosted digital data is seemingly immune from Fourth Amendment protection under the *Katz* line of cases, creating problems far broader than those in CSAM cases.[167]

IV. THE THIRD-PARTY PROBLEM IN CSAM CASES

Since *Katz*, and especially in the Internet Era, courts continue to struggle with the troublesome third-party doctrine.[168] Third-party services providers host virtually all online digital data in the 21st century.[169] This has inexorably led to an

158. *See id.* at 397 ("The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud. Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house. But officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.").

159. *See infra* Subsection VI.A.3 (highlighting the current tension on the Court post-*Carpenter*).

160. *See* United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016) (examining the unique nature of hash scanning "in light of *Jones*" and finding it "at least possible the [Supreme] Court today would find that a 'search' did take place").

161. Ian Paul, *Getting Started with Signal and Other Encrypted Messaging Apps*, PC WORLD (Mar. 11, 2021), https://www.pcworld.com/article/3610397/what-is-signal-encrypted-messaging-app.html (on file with the *University of the Pacific Law Review*).

162. *Id.*

163. *Id.*

164. *See id.* ("Encrypted messaging services are a great way to keep private information private with apps that are very easy to use.").

165. S*ee, e.g.*, 740 ILL. COMP. STAT. 14 §§ 5–20 (West 2021) (providing Illinois residents with similar rights over the use, transfer, and deletion of their online biometric data—including availability of civil damages for misappropriation).

166. *Supra* Section II.D.

167. *See supra* Section III.A (discussing the third-party doctrine's tendency to impinge on property and privacy rights).

168. *See supra* note 29.

169. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) (describing the quantity and quality of data that third-party service providers access).

erosion of what persons can realistically expect as far as the privacy of their data.[170] Further complicating that analysis is the expansion-of-the-search doctrine, which creates an oddity in investigating CSAM as *Ackerman* makes clear.[171]

Section A introduces the *Burdeau* rule, which stands for the proposition that private-party searches typically do not implicate the Fourth Amendment.[172] Section B discusses a key Supreme Court decision dealing with a private-party search where the entity then passed the results of that search on to federal agents.[173] Section C introduces the problems inherent in the third-party doctrine and shows the dramatically different outcomes that can arise if the government expands upon a private search.[174]

A. Private-Party Searches and the Burdeau Rule

In an early 20th century opinion, the Supreme Court laid down its general approach to limiting Fourth Amendment protection to only those searches that government agencies conduct.[175] Law enforcement cites the Court's opinion in *Burdeau* with regularity—dubbed the "*Burdeau* rule"—sidestepping Fourth Amendment protection when a private party acts "entirely independently of the government."[176] However, this bright line rule is not always controlling, especially when a private entity conducts a search for the government's benefit.[177] The Supreme Court eventually reached a middle ground, holding that private parties may indeed constitute "agents or instruments" of the government with sufficient governmental "involvement" or "encouragement."[178] Furthermore, some courts have held the scope of a private search may, as a constitutional corollary, directly limit law enforcement's subsequent search to that same scope.[179]

B. United States v. Jacobsen *and the Expansion Doctrine*

The Supreme Court has consistently interpreted the Fourth Amendment's protection against unreasonable searches "as proscribing only governmental

170. Vitiello, *supra* note 18, at 427.

171. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *infra* Section IV.C.

172. *Infra* Section IV.A.

173. *Infra* Section IV.B.

174. *Infra* Section IV.C.

175. *See* Burdeau v. McDowell, 256 U.S. 465, 476 (1921) (concluding that a private-party search—an employer—does not constitute a search under the Fourth Amendment).

176. Kosseff, *supra* note 14, at 194.

177. *Id.*

178. *See id.* at 196 (citing Skinner v. Ry. Lab. Executives' Ass'n, 489 U.S. 602 (1989)).

179. *Infra* Subsection IV.C.2.

action; it is wholly inapplicable to [private searches]."[180] Unless a private individual is "acting as an agent of the Government or with the participation or knowledge of [a] government official," the Fourth Amendment does not apply.[181] *Jacobsen* illustrates the third-party doctrine at work in a private-party physical search case that courts frequently cite in the non-governmental search context.[182]

In *Jacobsen*, FedEx employees were operating a forklift when one employee unintentionally damaged and tore open a package in the warehouse.[183] The employees then noticed a "white powdery substance" visible at the torn section of the package.[184] They called a federal narcotics agent who tested the powder, determining that it was cocaine.[185] Importantly, the agent needed only to look upon the package, which the employees had already torn open.[186] As the Court saw it, "[t]he initial invasions of [the] package were occasioned by private action," not the federal agent.[187]

The Court concluded that the federal agent's "additional invasions . . . must be tested by the degree to which they exceeded the scope of the private search."[188] This expansion-of-the-search theory comports with older precedent where the Court has flatly stated that it is not incumbent on the police to "avert their eyes."[189] The Court concluded that law enforcement had not violated Jacobsen's Fourth Amendment rights under either a privacy or property rights rationale.[190]

C. Problems of Agency and the Scope of Private Searches

Ackerman—which this Comment introduced at the outset—also presents unique questions about the intersection of the third-party doctrine and digital searches for CSAM.[191] This case brings into sharp relief the impact that an individual platform's "specific methods and procedures" for investigating CSAM have on subsequent judicial interpretation.[192] Depending on the methods a platform employs to investigate suspected CSAM, courts will either exclude or admit that

180. United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citing Walter v. United States, 447 U.S. 649, 662 (1980)).

181. *Id.*

182. *See* Kosseff, *supra* note 14, at 214–15 (highlighting the Supreme Court's focus "on the control that the government has exerted over the private-party's search").

183. *Jacobsen*, 466 U.S. at 111.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.* at 115.

188. *Id.* (citing Walter v. United States, 447 U.S. 649, 657 (1980)).

189. Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971).

190. *See Jacobsen*, 466 U.S. at 126 ("In sum, the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct. To the extent that a protected possessory interest was infringed, the infringement was *de minimis* and constitutionally reasonable.").

191. *Supra* Part I.

192. Kosseff, *supra* note 14, at 209.

evidence.[193] Put simply, the key distinction under the third-party rule is whether private companies have opened the data's *content*, or if it has only exposed its *metadata*.[194]

Subsection 1 discusses the *Ackerman* court's approach to agency theory, finding that the NCMEC qualifies as a governmental agent meaning that the Fourth Amendment applies to its activities.[195] Subsection 2 describes the prevailing view that the results of a private-party search with *opened content* will not typically implicate the Fourth Amendment.[196] Subsection 3 outlines the *Ackerman* problem where a private hash scan for CSAM, which AOL sent to the NCMEC with the content *unopened*, resulted in Fourth Amendment protection.[197]

1. Ackerman*: The NCMEC as a Governmental Agent*

The Tenth Circuit assessed whether the private nonprofit—the NCMEC—qualified as a "governmental entity" for purposes of the Fourth Amendment.[198] In so doing, the court looked to the statutory scheme, finding that Congress imposed requirements on both private companies and the NCMEC.[199] Further, Congress "permitted NCMEC to review Mr. Ackerman's email and attachments" and also "required [it] to pass along a report . . . to law enforcement."[200] Finally, the court cited *Skinner v. Railway Labor Executives' Association*, finding that Congress has provided "encouragement, endorsement, and participation" in the NCMEC's searches.[201] Therefore, at least the Tenth Circuit has concluded that the NCMEC qualifies as a governmental agent given its Congressional authorization and broad mandate under U.S. law.[202]

2. When the Government Does Not Expand upon the Private Search

Courts are not uniform in finding private parties' and the NCMEC's activities as implicating the Fourth Amendment search analysis.[203] The U.S. District Court for the District of Montana is just one example of a court that has sidestepped

193. *Id.*

194. *Id.*

195. *Infra* Subsection IV.C.1.

196. *Infra* Subsection IV.C.2.

197. *Infra* Subsection IV.C.3.

198. United States v. Ackerman, 831 F.3d 1292, 1295 (10th Cir. 2016).

199. *Id.* at 1302.

200. *Id.* at 1301–02.

201. *Id.* at 1302.

202. *Id. But see* Kosseff, *supra* note 14, at 214–15 (discussing then-Judge Gorsuch's purported "imprecise application" of the agency test to the NCMEC as improperly relying upon "subjective assessments" of the NCMEC's intent in investigating CSAM).

203. Kosseff, *supra* note 14, at 194.

Fourth Amendment search analysis in this context.[204] There, the court found that when Google employees open and review flagged images, law enforcement's *subsequent identical review* does not expand upon the initial private search.[205] The theory is in line with *Jacobsen*: the invasion of privacy has already taken place at the hands of the private entity—a software platform.[206] As the third party has already opened and viewed the content, the government's mere receipt of the results of that private search does not violate the Fourth Amendment.[207]

3. The Ackerman *Problem: When the Government Expands Upon the Private Search*

The secondary issue after agency in *Ackerman* was whether the NCMEC expanded upon AOL's initial search by opening and viewing the contents of Ackerman's email.[208] Importantly, when AOL's scan hit on a hash value match for CSAM, the analyst closed the account and submitted a report to the NCMEC.[209] This report included only "the email header information . . . IP address of the sender, and the IDFP hash value"—i.e., only the *metadata*.[210] At that point, the NCMEC took over the investigation and opened this digital container, confirming the existence of CSAM in Ackerman's original email.[211] The crux to these facts, as the Tenth Circuit was concerned, was AOL's failure to actually open and view the *content* of Ackerman's email.[212]

The first hurdle the court addressed was this expansion-of-the-search issue, stating that the NCMEC "exceeded rather than repeated AOL's private search."[213] In reaching this conclusion, the court distinguished *Jacobsen* where the agent discovered "nothing else of significance" that the FedEx employees had not already discovered—a white powder.[214] But on *Ackerman's* facts, the metadata container "*did* contain three additional [files], the content of which" AOL never ascertained.[215]

---

204. *See* United States v. Drivdahl, No. CR 13–18–H–DLC, 2014 WL 896734, at *4 (D. Mont. Mar. 6, 2014) (concluding that because "suspect material was opened by a Google employee prior to being turned over to the Government . . . there was no expansion of the private search which would have required a warrant").

205. *Id.*

206. *See supra* Section IV.A (describing the *Burdeau* rule and its special treatment of private-party searches and *Jacobsen* which describes the objective nature of the scope of the initial private-party search).

207. *Drivdahl*, 2014 WL 896734, at *4.

208. *See supra* Part I (introducing the key facts of *Ackerman*).

209. United States v. Ackerman, No. 13–10176–01–EFM, 2014 WL 2968164, at *3 (D. Kan. Jul. 1, 2014).

210. *Id.* at *3.

211. *Id.* at *3.

212. United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016).

213. *Id.*

214. United States v. Jacobsen, 466 U.S. 109, 119 (1984).

215. *Ackerman*, 831 F.3d at 1306.

The court also analogized digital email and the files within to physical mail parcels.[216] The majority reasoned, "after all, if opening and reviewing 'physical' mail is generally a 'search'—and it is—why not 'virtual' mail too?"[217] It also mentioned the "so-called 'third-party doctrine'" and its likely limitations in the digital email context—but resolved the search issue on the scope of the initial search.[218] Finally, the court took further pains to make mention of the Fourth Amendment's "original meaning" as explicated in *United States v. Jones*.[219] "Government conduct can constitute a Fourth Amendment search *either* when it infringes on a reasonable expectation of privacy *or* when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effects")."[220]

To the Tenth Circuit, a property-focused Fourth Amendment may afford *more protection* to digital data than the *Katz* privacy model.[221] Private email searches "see[m] pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment."[222] Whether hash value scans fall on the *Jacobsen* or *Jones* side of the line is a matter that the Supreme Court has yet to take up.[223] But with Judge Gorsuch now on the Court, the seemingly stricter property rights interpretation to digital data may influence the outcome.[224]

Courts should not incentivize platforms to open and view users' content as the expansion-of-the-search doctrine seems to make a requirement.[225] This is especially important when that content is imagery depicting the sometimes violent sexual exploitation of children.[226] Instead, hash scanning's "less than one in one billion" chance of incorrectly flagging CSAM should create the probable cause

---

216. *Id.* at 1304 (10th Cir. 2016).

217. *Id.*

218. *Id.*

219. *Id.* at 1307; *see* United States v. Jones, 565 U.S. 400 (2012) (describing the Fourth Amendment's "original meaning" as focused on "a particular concern for government trespass upon the areas ("persons, houses, papers, and effects")" it enumerates, and also adding that "Fourth Amendment rights do not rise or fall with the *Katz* formulation").

220. *Ackerman*, 831 F.3d at 1307.

221. *Id.*

222. *Id.*

223. *See* United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009) (pondering whether the Supreme Court is likely to take up a hash scanning case in light of the prevalence of the practice).

224. *See infra* Subsection VI.A.3 (describing the current tension on the Supreme Court between the seemingly competing privacy and property rationales).

225. *See Ackerman*, 831 F.3d at 1306 (finding a governmental search where the private entity service provider did not first open the content of an email prior to reporting the hash scan match to law enforcement).

226. Michael C. Seto, et al., *Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims*, NCMEC, 1, 3 (2018) https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf (on file with the *University of the Pacific Law Review*).

necessary to enable law enforcement to conduct a digital content search.[227] And this is exactly what AOL did in *Ackerman*.[228] This approach limits the "human impact on front-line safety teams" who, under *Ackerman*, must view this traumatizing content for law enforcement to commence a successful prosecution.[229] *Ackerman*'s private-party search analysis creates a paradigm where technical minutia dictate which private searches will implicate the protections of the Fourth Amendment.[230]

Alternatively, instead of the privacy model's third-party doctrine, under a property-based formulation whether metadata alone qualifies for protection is an open question.[231] But analogues exist for an exception for metadata as beyond a property or privacy rights rationale.[232] Fortunately, it seems unlikely that the current composition of the Supreme Court would agree with the result in *Ackerman*.[233] Hash scan matches should satisfy the probable cause standard irrespective of a technical expansion of the search given their virtually certain accuracy.[234]

V. THE PROPERTY LAW MODEL OF THE FOURTH AMENDMENT AND COMMON LAW ANALOGUES TO HASH SCANNING

Generally, the Fourth Amendment bars "unreasonable searches and seizures," further stating that "no [w]arrants shall issue but upon probable cause."[235] But the text of the amendment is deeply intertwined with private property rights, protecting against unwarranted governmental search and seizure of the people's "persons, houses, papers, and effects."[236] Courts have remained mostly faithful to the text on this point, typically affording Fourth Amendment protection only when a case implicates one of these four "places or things."[237] However, with the Internet's

227. *An Introduction to Hashing*, *supra* note 72.

228. United States v. Ackerman, No. 13–10176–01–EFM, 2014 WL 2968164, at *3 (D. Kan. Jul. 1, 2014).

229. *Ackerman*, 831 F.3d at 1304; *see Microsoft Expands PhotoDNA*, *supra* note 45 (arguing for "creating a reduced human impacts on front-line safety teams who have to view content" by automating this process instead).

230. *See supra* Section IV.C (describing the 10th Circuit's broad interpretation of what activities will cause a court to find that a private entity has acted as a government agent).

231. *See Ackerman*, 831 F.3d at 1306 (discussing similar "interesting questions" but deciding the merits of the case on the expansion-of-the-search theory).

232. *See infra* Part V (discussing several common law exceptions to the Fourth Amendment's search prohibitions that are analogous to hash scanning).

233. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (focusing on the "privacies of life" instead of a digital property-based approach).

234. *See An Introduction to Hashing*, *supra* note 73 (making clear the distinct certainty that hashes create for analysts, the NCMEC, and law enforcement).

235. U.S. CONST. amend. IV.

236. U.S. CONST. amend. IV.

237. KERR, *supra* note 21, manuscript at 6; *compare* United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that a tracking device which recorded *movements on a public roadway* was not a search, as the surveillance took place in "plain view"), *with* United States v. Karo, 468 U.S. 705, 716 (1984) (holding that a

ubiquitous reach into American life and the fact that third-party platforms host most Americans' online data, the Supreme Court is straying from *Katz*.[238]

In a seminal case in 1886, the Supreme Court articulated one of the earliest judicial interpretations of the Fourth Amendment.[239] In *Boyd v. United States*, the government sought to prosecute Boyd for violation of the Customs and Revenue Laws.[240] To accomplish the task, the government obtained a court order instructing Boyd to produce incriminating goods and documents.[241] The Supreme Court concluded the government had violated Boyd's Fourth Amendment rights by not obtaining a warrant before requisitioning his private property.[242]

This early case drew upon the Framers' distaste for the English practice of issuing general warrants that "authorized searches in any place, for any thing."[243] *Boyd* "laid the seeds of a property-rights interpretation" to the Fourth Amendment.[244] Specifically, the Court stated, "every invasion of private property, be it ever so minute, is a trespass."[245] While the Court has significantly revised its approach since this "first period" of Fourth Amendment analysis, the Framers' reverence for individual property rights is the amendment's chief cornerstone.[246]

More recently, the Supreme Court has increased its focus on property law concepts in digital search case law and some Circuits have tracked this trend.[247] This is especially true as technology "has eroded privacy expectations," as anything one hosts on a third-party platform is subject to private scans and searches.[248] In *Ackerman*, the court highlighted the Framers' intended "protection of physical rather than virtual correspondence," but acknowledged "a more obvious analogy from principle to new technology is hard to imagine."[249] As this Comment has introduced, several state legislatures have already moved toward the approach of treating online data as personal property.[250] Moreover, Congress has

---

similar tracking device to that used in Knotts *which recorded activity inside the suspect's home* was a search because it was "[i]ndiscriminate monitoring of property that has been withdrawn from public view").

238. *See supra* Part III (discussing the evolution of what constitutes a protected thing, from paper records to metadata to geolocation data).

239. DRESSLER, *supra* note 119, at 91.

240. Boyd v. United States, 116 U.S. 616, 617 (1886).

241. *Id.*

242. *See id.* at 627 ("According to this reasoning, it is now incumbent upon the defendants to show the law by which this seizure is warranted. If that cannot be done, it is a trespass.").

243. *Id.* at 641.

244. DRESSLER, *supra* note 119, at 91.

245. *Boyd*, 116 U.S. at 627; DRESSLER, *supra* note 119, at 91.

246. DRESSLER, *supra* note 119, at 91; *see supra* section III (discussing the privacy rights revolution in Fourth Amendment law, expanding upon the property rights foundation).

247. Carpenter v. United States, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting) (describing cases like *Smith* and *Miller* as cases that—under a *Katz* analysis—"extinguish Fourth Amendment interests once records are given to a third party," whereas, "property law may preserve them").

248. Vitiello, *supra* note 18, at 427; *supra* Section IV.C.

249. United States v. Ackerman, 831 F.3d 1292, 1308 (10th Cir. 2016).

250. *See supra* note 34.

also hearkened to notions of theft and trespass in drafting its own anti-hacking, misappropriation, and trade secrets legislation.[251]

Yet, neither a privacy- or property-minded orientation in legislatures and the judiciary need impede investigators' successful prosecution of persons who traffic in CSAM.[252] As the Court of Appeals for the Tenth Circuit concluded in *Ackerman*, an email header or recipient address—for example—is merely a "virtual container."[253] And a common thread in Supreme Court search law analysis is that mere containers do not typically enjoy Fourth Amendment protection; their *contents* are another matter.[254]

Section A describes a focal point for the property law approach in a recent digital search case, which seems to edge the Court away from *Katz*.[255] Section B introduces the unique, "*sui generis*," common law search doctrine of narcotics dog sniffs as an analogue to digital hash scans.[256] Section C reintroduces the plain view doctrine and argues that metadata—at least in the hash scan context—should come within plain view.[257] Section D analogizes hash scans to the Supreme Court's long embraced *Terry* pat down case law.[258]

A. United States v. Jones*: The Trespassory Test*

In *United States v. Jones*, the Supreme Court reinfused its Fourth Amendment search jurisprudence with time-honored property law concepts.[259] The case involved an FBI and local police agency task force tracking a suspect's geolocation with a GPS tracking device that they had physically attached to his vehicle.[260] Crucial to the Court's reasoning was the fact that the police committed a "classic trespassory search" when they physically placed the GPS device on the vehicle.[261]

---

251. *See, e.g.*, Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030(a)(4) (prohibiting the unauthorized access to a computer system to "obtain anything of value").

252. *See supra* Part V (arguing for several approaches courts could take to allow a hashing exception to search analysis).

253. *Ackerman*, 831 F.3d at 1307 (explaining that the "Fourth Amendment's original meaning," as explained by *Jones*, is that the government can conduct a "Fourth Amendment search *either* when it infringes on a reasonable expectation of privacy *or* when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing").

254. *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 13 (1977) (emphasis added) ("luggage *contents* are not open to public view . . . [further] luggage is intended as a repository of personal effects"); United States v. Place, 462 U.S. 696, 707 (1983) ("A 'canine sniff' by a well-trained narcotics detection dog, however, does not require opening the luggage.").

255. *Infra* Section V.A.

256. *Infra* Section V.B.

257. *Infra* Section V.C.

258. *Infra* Section V.D.

259. *See* United States v. Jones, 565 U.S. 400, 405 (2012) ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous.").

260. *Id.* at 402.

261. *Id.* at 412.

Writing for the majority, Justice Scalia critiqued *Katz*, stating it "did not snuff out the previously recognized protection for property."[262] Justice Scalia further highlighted that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, but not *substituted for*, the common-law trespassory test."[263] Justice Sotomayor in concurrence offered the caveat that the "technological advances that have made possible nontrespassory surveillance techniques" clearly reduce societal expectations of privacy.[264] Speaking for herself, she described the *Katz* corollary doctrines as "ill suited to the digital age" given the quantity of information Americans give to third parties.[265] Ultimately, she embraced Scalia's formulation as a "narrower basis for decision" and found the police trespass alone as dispositive of the constitutional violation.[266]

Interestingly, the Court also stated in dicta that "situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."[267] This would seem to indicate that mere hash scanning, especially where a platform does not open actual content, would not rise to the level of a trespass.[268] It is also "minimally intrusive" when platforms scan for the unique identifiers hash values contain, indicating that such scans fall outside the narrower property formulation.[269] Hence, hash scanning sidesteps the property analysis given its lack of trespass, its precise application, and its lack of content exposure.[270] Finally, while the Court indicated that analyzing mere "electronic signals" would remain firmly in the *Katz* rubric, this ignores other readily analogous common law concepts.[271]

B. United States v. Place*: The Sui Generis Search*

Place provides that a canine sniff is "so limited" both in scope and in the "information revealed" that it does not constitute a search under the Fourth Amendment.[272] Similarly, in CSAM investigations it is the virtual container itself

262. *Id.* at 407.

263. *Id.* at 409.

264. *Id.* at 415.

265. *United States v. Jones*, 565 U.S. at 417.

266. *Id.* at 418.

267. *Id.* at 411.

268. *Id.* at 411.

269. United States v. Place, 462 U.S. 696, 707, 709 (1983) ("[D]espite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited.").

270. *See An Introduction to Hashing*, *supra* note 73 (discussing a hash scan's "less than one in one billion" chance of a false positive as well as its lack of content exposure).

271. *See infra* Sections V.B–D (arguing for the applicability of multiple common law analogues to hash scanning).

272. *Place*, 462 U.S. at 707; *compare* Illinois v. Caballes, 543 U.S. 405, 409 (2005) (quoting *Place*) ("[T]he use of a well-trained narcotics-detection dog—'one that does not expose noncontraband items that otherwise would remain hidden from public view,'—during a lawful traffic stop, generally does not implicate legitimate

that affords the requisite probable cause—the hash value of the scanned file.[273] The content remains unexposed, much like narcotics hidden from view inside of a briefcase that only a dog sniff can discover.[274] Such investigatory methods the Court in *Place* found to be "*sui generis*" and beyond the reach of Fourth Amendment protection.[275] Hash scanning similarly preserves the other "privacies" contained within source files, but like a dog sniff, "the information obtained is limited."[276] Furthermore, no physical intrusion or "classic trespass[]" occurs when platforms scan for these proprietary metadata files.[277] This common law doctrine, for hash scanning at least, is a ready alternative to an otherwise cumbersome and invasive third-party doctrine rule.[278]

C. The Plain View Exception

Similarly, plain view to metadata provides another avenue for courts to legitimize hash scans, which courts have applied when there was evidence that "crime was afoot."[279] As this Comment discussed above, the near certainty that a hash scan affords to platforms and law enforcement without exposing content brings such metadata within plain view.[280]

Another core Fourth Amendment requirement is the necessity that any warrant "particularly describ[e] the place to be searched, and the persons or things to be seized."[281] The majority in *Horton v. California* saw the particularity requirement as one that "serves primarily as a protection against unjustified intrusions on privacy."[282] Yet, the dissent more comprehensively described this requirement as reflecting the Fourth Amendment's aim of protecting "privacy and possessory interests" as "equally important."[283]

---

privacy interests."); *with* Kyllo v. United States, 533 U.S. 27, 37 (2001) (concluding that law enforcement's use of a thermal-imaging device to detect only marijuana cultivation in the home constitutes a Fourth Amendment search because government "intrusion into a constitutionally protected area,"—the home—invades a sphere where "*all* details are intimate details").

273. *See An Introduction to Hashing*, *supra* note 73 (describing hash scanning's virtually certain "one in one billion" chance of misidentifying CSAM, far exceeding the probable cause standard).

274. *See Place*, 462 U.S. at 707 ("[D]espite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited.").

275. *Id.*

276. *Id.*; *see also Caballes*, 543 U.S. at 410 ("The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection [by dog sniff] of contraband in the trunk of his car. A dog sniff conducted during a concededly lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment.").

277. United States v. Jones, 565 U.S. 400, 412 (2012).

278. *See supra* Part IV (discussing the problems with the third-party doctrine).

279. DRESSLER, *supra* note 119, at 403.

280. *See Place*, 462 U.S. at 707 ("[D]espite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited.").

281. U.S. CONST. amend. IV.

282. Horton v. California, 496 U.S. 128, 141 (1990).

283. *Id.* at 143 (Brennan, J., dissenting).

A noted exception to the warrant requirement is the plain view doctrine.[284] The Supreme Court described plain view in *Horton* as requiring two basic components.[285] First, the item must be in plain view, but the incriminating character of the evidence must be "immediately apparent."[286] Second, the officer must "have a lawful right of access to the object itself."[287] The Court also highlighted that "law enforcement is best achieved by the application of objective standards of conduct," not subjective states of mind.[288]

In one CSAM case, the Court of Appeals for the Fourth Circuit went so far as to say that searching "computer and electronic media" files may fall within plain view.[289] The court reached this result given there was a warrant describing tangible, physical mediums located in the defendant's home.[290] The court reasoned the warrant "impliedly" authorized the police to "open each file on the computer and view its contents" to ascertain its illicit nature.[291] In sum, the warrant authorized opening files on the computer, which meant any illegal content police encountered during that search was also within the warrant's scope.[292]

The Court of Appeals for the Tenth Circuit took a different approach in an earlier CSAM case in *United States v. Carey*.[293] The court called the plain view approach "intriguing," but declined to embrace it.[294] It reasoned that "[a]nalogies to [physical] containers . . . may lead courts to 'oversimplify a complex area . . . and ignore the realities of massive modern computer storage.'"[295] Ten years later in *United States v. Burgess*, the Tenth Circuit continued to struggle with the question "given [digital sources'] unique ability to hold vast amounts" of data.[296] The court continued, "one might speculate whether the Supreme Court would treat laptop computers, hard drives, flash drives or even cell phones as it has [physical containers]."[297] Ultimately, the *Burgess* court dodged the question, concluding that

284. *See id.* at 136 (concluding that: (1) the item must be in "plain view;" (2) "it's incriminating character must also be 'immediately apparent;'" and (3) "the officer must have a lawful right of access to the object itself.").

285. *Id.*

286. *Id.*

287. *Id.* at 137.

288. *Horton*, 496 U.S. at 138.

289. United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010).

290. *Id.* at 515–16 (warranting a search and seizure of: "[a]ny and all computer systems and digital storage media, videotapes, videotape recorders, documents, photographs, and Instrumentalities indicat[ive] of the offense of . . . Harassment by Computer . . . .").

291. *Id.* at 522.

292. *Id.*

293. *See* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (declining to embrace the plain view exception to the warrant requirement).

294. *Id.*

295. *Id.* at 1275.

296. United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009).

297. *Id.*

the warrant to search the defendant's mobile home included authorization to search any computer files in his hard drives.[298]

For CSAM investigations, courts should view hash scanning as satisfying the two-fold requirement outlined in *Horton*.[299] First, when a scan confirms a positive hash value match, that result borders on near certainty—exceeding the probable cause standard.[300] Second, platforms hosting data transfers—where they disclose their scanning activities—have a "lawful right of access to the object," meaning, the hashes.[301] This is not to suggest that platforms have such "right of access" to the *content of communications*, but the container housing it on their network is qualitatively different.[302] Many end user license agreements specify that platforms may scan, screen, or remove data that analysts find to be objectionable under company policy or existing law.[303]

Finally, the Supreme Court has made clear that "plain view alone is never enough" for evidence seizure.[304] But with hash scanning, there are two distinct components to such scans that bring them within plain view.[305] First, the platforms have a right of access to the data container itself—the hash value.[306] And second, it is not simply the platforms *viewing* of the metadata that creates probable cause.[307] The scan's *corroboration* with other verified CSAM files is what prompts analysts to escalate the report to law enforcement.[308] Hence, it is not plain view alone, but plain view with virtually certain corroboration to that particular file.[309]

---

298. *Id.*

299. Horton v. California, 496 U.S. 128, 136–37 (1990).

300. *See An Introduction to Hashing*, *supra* note 73 (describing has sequences as "so distinct that the chance that any two data sets are given the same hash value is less than one in one billion").

301. *Horton*, 496 U.S. at 137.

302. *See What Is a Hash?*, *supra* note 25 (discussing the unique features of a hash value that do not expose users' personal data).

303. *See, e.g.*, WELCOME TO ICLOUD: APPLE LEGAL SERVICE AGREEMENT, https://www.apple.com/legal/internet-services/itunes/us/terms.html (last visited June 3, 2021) (on file with the *University of the Pacific Law Review*) ("Apple may monitor and decide to remove or edit any submitted material. Submissions Guidelines: You may not use the Services to . . . post objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content."); *see also Expanded Protections for Children*, APPLE, https://www.apple.com/child-safety/ (last visited Sept. 1, 2021) (on file with the *University of the Pacific Law Review*) (introducing Apple's new "ambitious" hashing software that has scanning capabilities on all Apple user's iCloud photo streams and physical devices for CSAM). *But see* Brian Barrett & Lily Hay Newman, *Apple Backs Down on Its Controversial Photo-Scanning Plans*, WIRED (Sept. 3, 2021, 12:58 PM), https://www.wired.com/story/apple-icloud-photo-scan-csam-pause-backlash/ (on file with the *University of the Pacific Law Review*) ("The backlash from cryptographers to privacy advocates to Edward Snowden himself was near-instantaneous . . . . After weeks of sustained outcry, Apple is standing down. At least for now.").

304. Coolidge v. New Hampshire, 403 U.S. 443, 468 (1971).

305. *See supra* Section II.C (describing the technical process of hashing that does not implicate user's private data).

306. *See, e.g.*, WELCOME TO ICLOUD, *supra* note 303 (providing just one example of a legal terms of service agreement whereby platforms may scan and remove content that violates legal or contractual obligations).

307. *See* Salgado, *supra* note 12, at 40 (highlighting the hashing process as a corroboration of previously stored hashes—bringing the level of certainty to near perfection).

308. *Safer's Detection Technology*, *supra* note 68.

309. *An Introduction to Hashing*, *supra* note 73.

In sum, plain view does indeed present "intriguing" challenges in the era of massive online data storage.[310] And in the context of CSAM investigations, police and platforms should not have carte blanche to freely peruse users' *content*.[311] Courts should limit the scope of plain view to *only the data containers*—hash values—of such content, and only upon a hash scan match.[312] Furthermore, it should behoove companies to clearly disclose their hash scanning policies because they do not always do so.[313] Admittedly, many companies would consider such a judicial approach as justification to move to full end-to-end encryption on their platforms.[314] But the benefits of a judicial application of plain view to hashing would be immediate and within the limits of existing law.[315]

D. A Terry *Digital "Pat Down"*

Yet another common law analogue to hash scans is the *Terry* frisk procedure.[316] *Terry v. Ohio* stands for the proposition that police may conduct a cursory "pat down" of a suspect for weapons when they reasonably suspect danger.[317] This "search" must be "strictly tied to and justified by the circumstances which rendered its initiation permissible."[318] The Court of Appeals for the Eleventh Circuit concluded that where an officer "immediately recognize[d]" an item during a pat down as dangerous, no Fourth Amendment protection applied.[319] As a limiting principle however, *Terry* applies in a police officer's search for weapons or when an officer is investigating an already "completed felony."[320] In a weapons search, the risk of physical harm to the officer is balanced against the suspect's

310. United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

311. *See* United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016) (highlighting how personal email accounts, as one example, store "all sorts of private and personal details" including "perfectly legal images").

312. *See id.* (describing email as a "virtual container").

313. *See supra* note 303 ('discussing the controversy that openly disclosing hashing policies has created for Apple in 2021).

314. *See infra* Subsection VI.A.3 (describing the implications of current legal trends leading platforms to move to full encryption).

315. *See infra* Subsection IV.C.2 (discussing the formalistic distinctions courts currently make between when a search has, or has not, occurred).

316. *See* Terry v. Ohio, 392 U.S. 1, 30 (1968) ("[W]here a police officer observes unusual conduct which leads him reasonably to conclude . . . that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous . . . he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him.").

317. *See id.* ("Such a search is a reasonable search under the Fourth Amendment").

318. *Id.* at 17 (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967)).

319. United States v. Johnson, 921 F.3d 991, 999, 999 (11th Cir. 2019).

320. *See* DRESSLER, *supra* note 119, at 403 (citing United States v. Hensley, 469 U.S. 221 (1985) ("[T]he Court unanimously ruled that the *Terry* doctrine also applies when an officer seeks to investigate a *completed* felony: Brief seizures are allowed if the 'police have a reasonable suspicion, grounded in specific and articulable facts, that a person they encounter was involved in or is wanted in connection with a completed felony.'").

"personal security." *Terry* acknowledged the "great indignity" of such pat downs, given the highly intrusive nature of an officer's physical manipulation of a suspect's corporeal person.[321]

In completed felony searches, a hash scan provides *virtually certain* proof of the existence of CSAM in transfer—undoubtedly a felony act—with proof that surpasses the "reasonable suspicion" required by *Hensley*.[322] At the same time, law enforcement's intrusion upon the "sanctity of the person" is not present in a hash search.[323] The limited scope of a hash scan's reach into a person's "digital life" is also extremely narrow.[324] In this way, hash scans are essentially a private-party digital pat down—with probable cause—the results of which the private party lawfully hands off to law enforcement.[325]

Finally, under such formulations, whether platforms open the content or not, should make no difference once a hash scan creates probable cause.[326] No trespass occurs when companies merely scan the proprietary source code of a transferred file—leaving its content unexposed.[327] It is more like viewing the sender, recipient, and address information contained on the letterhead of physical mail parcel than it is to tearing open the letter itself.[328] These common law analogues avoid the unnecessary technicalities inherent in the third-party doctrine and recognize the narrow nature of hash scanning while preserving private property rights.[329]

VI. THE CURRENT FLUX OF TECHNOLOGY SEARCH CASE LAW

The legal mechanisms and modern trends outlined above present unique challenges to courts and companies that implicate broad policy considerations.[330] Current trends indicate that it is unavoidable that government agencies will not be in the best position to investigate CSAM and other digital crimes.[331] Platforms such as Facebook, Amazon, Apple, and Microsoft are the true gatekeepers of

321. Terry v. Ohio, 392 U.S. 1, 17 (1968).

322. *An Introduction to Hashing*, *supra* note 73; *see* DRESSLER, *supra* note 119, at 403 (describing the "completed felony" rule from *Hensley*).

323. *Terry v. Ohio*, 392 U.S. at 17.

324. *See supra* Section II.C (describing the sharply circumscribed nature of a hash scan).

325. *See Terry v. Ohio*, 392 U.S. at 30 (concluding that officers are entitled to "conduct a carefully limited search of the outer clothing of . . . persons").

326. *See* United States v. Drivdahl, No. CR 13–18–H–DLC, 2014 WL 896734, at *4 (D. Mont. Mar. 6, 2014) (reaching the correct result, albeit, given the Google employee's actual opening of the content).

327. *What Is a Hash?*, *supra* note 25.

328. United States v. Ackerman, 831 F.3d 1292, 1304 (10th Cir. 2016).

329. *Supra* Part V.

330. *Supra* Parts II–V.

331. *See supra* Section II.C (describing the process by which private company platforms host and scan data).

Americans' personal data.[332] Any legislative or judicial solutions to investigating CSAM requires this simple acknowledgment.[333]

As the *Katz* Court declared, "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[334] As technological advancement seemingly renders this phrase obsolete, the doctrine has come under serious assault.[335] In the recent decision *Carpenter v. United States*, the Court commenced a course leading to an inevitable collision between Americans' data privacy rights and the troublesome third-party doctrine.[336]

Like *Riley* four years prior, *Carpenter v. United States* signaled the Supreme Court's continued attempt at modernizing the traditional *Katz* property-plus-privacy approach.[337] The FBI arrested Carpenter for suspicion of taking part in a string of robberies in Detroit, Michigan.[338] FBI agents interrogated the suspect, and he revealed the names and cell phone numbers of several of his accomplices.[339] Under the Stored Communications Act, agents applied for court orders to obtain cell-site location information ("CSLI") from cell phone service providers for each of the divulged numbers.[340] Armed with these warrants and service provider acquiescence, the FBI was able to track Carpenter's accomplices' previously logged movements using detailed geographic data.[341]

The Court noted, "property rights are not the sole measure of Fourth Amendment violations" yet also specifically "decline[d] to extend *Smith* and *Miller* to cover these novel circumstances."[342] So the Court, while unwilling to embrace property law concepts, also explicitly declined to extend the troublesome third-party doctrine.[343]

---

332. *See Microsoft Expands PhotoDNA*, *supra* note 45 (discussing Microsoft's role with "over 70 companies" combatting the proliferation of CSAM on their platforms).

333. *See id.* (highlighting the effectiveness of private platform's tools—like PhotoDNA—for scanning and isolating illicit content).

334. Katz v. United States, 389 U.S. 347, 351 (1967).

335. *See supra* note 29. *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 601 (2009) ("The importance of third-party records in new technologies and the continuing criticisms of the Court's case law suggest that the time has come for courts and commentators alike to develop a more sophisticated understanding of the third-party doctrine. The doctrine should be recast rather than cast aside.").

336. *See infra* Subsection VI.A.3 (discussing *Carpenter's* shift away from expectations of privacy and the third-party doctrine, embracing instead the goal of securing "the privacies of life against arbitrary power" and inhibiting "a too permeating police surveillance").

337. KERR, *supra* note 21, manuscript at 6.

338. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

339. *Id.*

340. *Id.* at 2212–13.

341. *Id.* at 2212.

342. *Id.* at 2213, 2217.

343. *Id.* at 2217.

The Court also took special note of the type of metadata at issue—location data that "hold for many Americans the privacies of life."[344] Specifically, governmental monitoring of CSLI data "over the course of 127 days provides an all-encompassing record of the holder's whereabouts."[345] The majority viewed this type of data as "near perfect surveillance"—likening it to an ankle monitor on the phone's user.[346]

In contrast, the dissent observed the Court "unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded" search law analysis.[347] Moreover, Justice Gorsuch noted *Katz* has spawned such troublesome search law issues like the third-party doctrine—as the Court introduced in *Smith* and *Miller*.[348] Rather, he and at least three other Justices would instead lean into a property-based formulation of the Fourth Amendment in the digital data context.[349] To Justice Gorsuch, it seems "entirely possible that a person's cell-site location data could qualify as *his* papers or effects under existing law."[350]

Whichever direction the Court proceeds in the wake of *Carpenter* remains unclear.[351] Yet, hash scanning provides a means by which CSAM investigations and private-party searches pass constitutional muster under either model.[352] On the one hand, the digital container itself has truncated Fourth Amendment protection under a strict property law formulation given that hash scans reveal no content.[353] At the same time, the discreteness of such scans does not impinge upon the "privacies of life" as the majority was concerned with in *Carpenter*.[354] Furthermore, the metadata that a hash scan reveals does not implicate the concerns that the Court addressed in *Carpenter*—in neither quality or duration of surveillance.[355]

Finally, it is an open question on where the Court is likely to take the third-party doctrine in the wake of cloud storage and peer-to-peer networking.[356] But

344. *Carpenter*, 138 S. Ct. at 2217 (citing Riley v. California, 573 U.S. 373, 403 (2014)).

345. *Id.*

346. *Id.* at 2218.

347. *Id.* at 2224 (Kennedy, J., dissenting).

348. *Id.* at 2262 (Gorsuch, J., dissenting).

349. *Id.* at 2223 (Kennedy, J., Alito, J., & Thomas, J., dissenting), *Carpenter*, 138 S. Ct. at 2261 (Gorsuch, J., dissenting).

350. *Id.* at 2272.

351. *See* KERR, *supra* note 21, manuscript: abstract ("*Carpenter* prompts fundamental questions of what the Fourth Amendment means in the digital age.").

352. *See supra* Parts III–V (arguing for the constitutionality of hash scans under either model of the Fourth Amendment).

353. *Safer's Detection Technology*, *supra* note 68.

354. *Carpenter*, 138 S. Ct. at 2210, 2217 (citing Riley v. California, 573 U.S. 373, 403 (2014)).

355. *See id.* at 2217 ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations.").

356. *See generally* KERR, *supra* note 21, manuscript at 1 (arguing that the Justice's "instincts are right" in creating the "*Carpenter* shift," but that that decision was "premature" and "laid the groundwork for the similar

what is clear is that the privacy model's embrace of "diminished expectations of privacy" for information given to third parties is entirely untenable in the current paradigm.[357] Property and common law concepts may in fact provide less intrusive ways of both protecting personal data and allowing for precise investigation tools like hash scanning.[358]

VII. CONCLUSION

American society and technological advancement have come a long way since *Katz*.[359] Individuals' expectations of privacy have—quite reasonably—eroded in data that they create, post, and share online.[360] While *Katz* was meant to broaden Fourth Amendment protection beyond the traditional limits of "constitutionally protected area[s]," treating *digital* data as property may further "preserve them."[361] To be sure, the "*Carpenter* shift" may well afford more strenuous digital data protections, but *Carpenter* also "requires line drawing where no obvious lines exist."[362]

American common law has more clearly established the contours of property law in the context of the Fourth Amendment.[363] The Supreme Court is poised to abandon the troublesome *Katz*-corollary doctrines enunciated in *Smith* and *Miller*, as those holdings have lost their force in the digital era.[364] Perhaps counterintuitively, it is the more archaic rules of trespass and property rights in the technology search context that may afford greater protection within existing law.[365] Yet, under even a narrower property-based model of the Fourth Amendment,

---

treatment of digital technologies present and future that genuinely raise the concerns the Justices expressed in *Carpenter*.").

357. *Carpenter*, 138 S. Ct. at 2246 (Thomas, J., dissenting) ("[T]he *Katz* test is a failed experiment"); *id.* at 2264, 2272 (Gorsuch, J., dissenting) ("In the end, what to *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants . . . Mr. Carpenter pursued only a *Katz* 'reasonable expectations' argument. He did not invoke the law of property or any analogies to the common law . . . [he] forfeited perhaps his most promising line of argument").

358. *Supra* Part V.

359. *See generally* Katz v. United States, 389 U.S. 347 (1967) (decided on the factual scenario of the case dealing with existing technology in the 1960s—telephone booths).

360. Vitiello, *supra* note 18, at 427.

361. *Katz v. United States*, 389 U.S. at 350; Carpenter v. United States, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J., dissenting).

362. KERR, *supra* note 21, manuscript at 2.

363. *See supra* Part V (discussing important property law concepts in the digital context).

364. Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018) (reasoning for the majority that *Smith* and *Miller* may not "exten[d] to the qualitatively different category of cell-site records"); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g.*, *Smith* [and] *Miller*. This approach is ill-suited to the digital age.").

365. *See supra* Part IV (arguing for a more tailored common law approach to protecting digital content yet allowing for hash scanning).

hashing presents a unique method of locating and isolating content that is unequivocally unlawful.[366]

Ultimately, confirmed metadata scans highly corroborative of CSAM should allow tech companies to provide only the metadata to government agencies for review.[367] Courts should not find preliminary hash scanning to be a governmental search given the uniquely circumscribed nature—and virtual certainty—of the scan.[368] Furthermore, private companies should not be the entities who actually open and view such content.[369] Before a content search takes place, third parties' provision to law enforcement of the *metadata* should establish warranted probable cause to search that transmission's *content.*[370] This Comment's analysis of hash scanning affords the most protection for users' data, shields unnecessary exposure to third parties, and avoids undesirable results like *Ackerman*.[371]

366. *See, e.g.*, United States v. Place, 462 U.S. 696, 707 (1983) (concluding that when "the information obtained is limited" the scope of the Fourth Amendment protection is limited as well).

367. *See supra* Subsection IV.C.2 (arguing that the result in *Ackerman* should be avoided).

368. *An Introduction to Hashing*, *supra* note 73.

369. *See Microsoft Expands PhotoDNA*, *supra* note 45 (arguing for "creating a reduced human impacts on front-line safety teams who have to view content" by automating this process instead).

370. *See supra* Part IV (arguing for this result under existing law).

371. *See supra* Subsection IV.C.2 (discussing the undesirable result in *Ackerman*); *Microsoft Expands PhotoDNA*, *supra* note 45.