Washington and Lee Journal of Civil Rights and Social Justice

Volume 30 | Issue 2 Article 12

Spring 2024

Skirting the Fourth Amendment: How Law Enforcement Agencies Abuse Technology and Constitutional Exceptions to Surveille the Public

Matthew Lloyd
Washington and Lee University School of Law, lloyd.m24@law.wlu.edu

Skirting the Fourth Amendment: How Law Enforcement Agencies Abuse Technology and Constitutional Exceptions to Surveille the Public

Matthew Lloyd*

Abstract

Existing Fourth Amendment law does not protect against law enforcement use of data gathered through the internet either by private companies who actively search their customer's data and submit evidence of misconduct to law enforcement or from private companies who acquire the data on behalf of law enforcement. In an effort to pursue criminals, courts have permitted Fourth Amendment jurisprudence to develop in a manner that permits sweeping invasions of privacy without any probable cause through the private search doctrine or without any procedural protections through the third-party doctrine. It will require substantial judicial or legislative action to return the level of privacy and security promised by the Fourth Amendment. Current law is split over whether to evaluate technology-based invasions using a human based approach that requires a human to actively participate in the invasions for them to be permissible or a statistics-based approach that permits invasions of privacy so long as there is a high statistical chance that contraband will not be misidentified. Providing citizens with security from the invasion itself has become lost in the debate over the correct way that a citizen's privacy should be warrantlessly invaded. The Supreme Court should stop the existing doctrines from applying to modern data collection because the existing legal framework was not designed, nor is able, to

* J.D. Candidate 2024, Washington and Lee School of Law. Professor Tim MacDonnell, thank you for your constant advice and guidance. Without your ability to identify connections across different areas of law, this Note would not have developed to nearly the same degree. I would also like to thank Rachel Silver for listening to my rants about the horrors of technology.

prevent improper invasions of data. Congress should pass national legislation to limit the ability of private actors to engage in reciprocal relationships with law enforcement where law enforcement receives information that would ordinarily require a warrant. For individual data to be granted the same protections that personal data had prior to the development of modern technology both Congress and the Supreme Court will need to take substantial steps.

Table of Contents

"To declare that, in the administration of the criminal law, the end justifies the means . . . would bring terrible retribution."[1]

"Privacy is not a discrete commodity."[2]

1. Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

2. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

I. Introduction.

Following Edward Snowden's infamous surveillance revelations, the PEW Research Center found that only six percent of people strongly believed that the government could keep their data safe.[3] In the time since that 2015 study, the government has not only failed to keep individuals' data safe, but has actively sought to acquire it without following the procedural safeguards provided by the United States Constitution.[4] The Fourth Amendment is the principle barrier that exists between sweeping government surveillance and the American public.[5] Yet, the effectiveness of this barrier is dependent on how courts interpret its terms. A concerning trend in Fourth Amendment jurisprudence is to tie the protections provided by the Amendment to the heinousness of a particular crime.[6] Turning a blind eye towards investigative practices that violate the core of the Fourth Amendment should be an easy error to avoid. However, that is not always the case when courts are facing strong evidence of a person possessing content relating to the exploitation of children. It is even rational to argue that, in cases involving victimized children, courts should do anything necessary to punish those responsible, including permitting illegal searches. The issue with such allowances is that the implications of the behavior are not limited to one case or prosecution. Under a precedent-based legal system, a court permitting certain investigative behaviors serves as an

3. *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RSCH. CTR. (May 20, 2015) (discussing the fact that the majority of Americans feel that privacy is very important) [perma.cc/R8M7-YLS6].

4. *See* Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget*,' AP NEWS (Sept. 2, 2022) (showing that a large number of law enforcement agencies are using a subscription service that functions as a cellphone tracking tool) [perma.cc/ZXE9-U6DN].

5. *See* Maryland v. King, 569 U.S. 435, 446–47 (2013) ("The Fourth Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner.") (referencing Schmerber v. California, 384 U.S. 757, 768 (1966)).

6. *See* State v. Mixton, 447 P.3d 829, 844–45 (Ariz. Ct. App. 2019) (permitting the good faith exception to allow for the use of evidence demonstrating the possession of child pornography that was gained from an improper warrant).

endorsement of them. An investigatory practice used to pursue child predators has nothing stopping it from being used against someone like a civil rights leader.[7] That is precisely what has occurred with respect to the private search doctrine.[8]

Modern technology is altering the threats to the Fourth Amendment, and the actions of private parties are rapidly becoming the driving factor behind Fourth Amendment concerns.[9] Private companies are increasingly willing to collect, examine, and sell information that citizens place on their laptops and cell phones.[10] Internet service providers are explicitly permitted to divulge individual data to other companies.[11] The only statutory protection offered to users is that internet service providers cannot knowingly provide customer information to the government.[12] That statutory protection is specifically qualified to permit disclosures to both the National Center for Missing and Exploited Children ("NCMEC") and law enforcement if the provider inadvertently obtained content that appears to pertain to the commission of a crime.[13] These exceptions trivialize the narrow statutory protections because the purpose behind privacy from government surveillance is intertwined with crime. The concern

7. *See* Benjamin Hedin, *The FBI's Surveillance of Martin Luther King, Jr. was Relentless. But Its Findings Paint a Fuller Picture for Historians*, TIME (Jan. 18, 2021) (noting that King was surveilled for more than four years due to the FBI Director's personal dislike of him) [perma.cc/KML7-L4W8].

8. *See* Jon Schuppe, *Police Sweep Google Searches to find Suspects. The Tactic is Facing its First Legal Challenge*, NBC (June 30, 2022) (discussing a case where a judge permitted law enforcement to search all users of Google to find anyone who searched for a specific address) [perma.cc/H9DM-5C2M].

9. *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019) (showing that private companies are conducting continuous surveillance on tens of millions of Americans) [perma.cc/SUU9-K5J9].

10. *See* Bennett Cyphers, *How the Federal Government Buys our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (June 13, 2022) (observing that various government agencies are participating in a partnership designed to surveil millions of people) [perma.cc/SJX6-ZKRA].

11. *See* 18 U.S.C. § 2702(c)(6) (permitting the disclosure of any record or other information pertaining to a customer to any person other than a governmental entity).

12. *See id.* § 2702(a)(3) (blocking an internet provider from divulging the records of user information to any governmental entity).

13. *See id.* § 2702(b)(6)–(7) (allowing the disclosures without additional limitations).

around privacy is not mockery by federal agents who uncover embarrassing information but that the government may use excessive surveillance to incarcerate individuals.

The laws preventing internet providers from giving information directly to the government do nothing to prevent internet providers from selling the same data to another party who intends to sell that information to the government.[14] This has caused the development of a data broker industry where companies package the data of millions of Americans and sell it to law enforcement.[15] No existing law prevents government organizations from acting as market participants.[16] The government's acquisition of private information is not a small problem. Federal agents are spending millions to purchase in-depth location data about Americans from companies who process fifteen billion location points from more than 250 million phones daily.[17] This information is so invasive that federal agents have been shown to voice objections to the practice even while continuing to make the purchases.[18] This process is particularly popular with local law enforcement because it does not require the

14. *See* Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People,"* 2009 COLUM. BUS. L. REV. 950, 977–98 (2009) (explaining that fourth-parties have the benefit of being free from Fourth Amendment and statutory concerns).

15. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REGUL. 595, 618–19 (2004) (noting that the inconsistent nature of United States privacy law creates substantial deficits in protection).

16. *See* Amitai Etzioni, *Reining in Private Agents*, 101 MINN. L. REV. 279, 286–87 (2016) (demonstrating that minimal privacy protections make it impossible to opt out of data collection and leave privacy merchant largely unregulated).

17. *See* Elizabeth Nolan Brown, *Homeland Security is Buying its Way Around the Fourth Amendment*, REASON (July 19, 2022) (discussing substantial data purchasing by DHS and various arguments by the ACLU) [perma.cc/5UC4-2R5T].

18. *See* Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, AM. C.L. UNION (July 18, 2022) (observing that internal emails showed both internal confusion about privacy and a temporary halt to data projects due to unanswered privacy and legal questions) [perma.cc/6J9A-K336].

paperwork that is usually required for surveillance of an individual or business.[19]

The desire to divulge user data is not always motivated by profit, but can include the desire to identify sexual predators.[20] In spite of the many goods that have come from the internet, it is undeniable that the internet has allowed for the propagation of substantial amounts of child pornography.[21] The material itself is heinous, and having a reputation for being a place where it is exchanged could be fatal to a business.[22] Hash-value matching is among the most effective technologies at identifying individuals who are trafficking in sexual content involving children.[23] Sexual conduct involving children can be discovered by a private company and sent to law enforcement due to an explicit statutory exception.[24]

The private search doctrine is a court created rule permitting government utilization of private searches including hash matched searches by internet companies.[25] This rule permits law

19. *See* Bennett Cyphers & Aaron Mackey, *Fog Data Science Puts our Fourth Amendment Rights up for Sale*, ELEC. FRONTIER FOUND. (Aug. 31, 2022) (remarking that members of multiple police departments were arguing that information from Fog Data Science required no paperwork because it comes from a company) [perma.cc/MT2M-DN9G].

20. *See* Reed Albergotti, *Apple is Prying into iPhones to Find Sexual Predators, but Privacy Activists Worry Governments Could Weaponize the Feature*, WASH. POST (Aug. 5, 2021) (discussing Apple's implementation of new software tools designed to target child pornography) [perma.cc/C69Z-QUM6].

21. *See What is Child Sexual Abuse Material (CSAM)*, RAPE, ABUSE & INCEST NAT'L NETWORK (Aug. 25, 2022) (noting that nearly 85 million images and videos of CSAM were reported in 2021 alone) [perma.cc/G5JA-3TTS].

22. *See* Emma Roth & Richard Lawler, *Google AI Flagged Parents' Accounts for Potential Abuse over Nude Photos of their Sick Kids*, THE VERGE (Aug. 21, 2022) (explaining that the fear of negative press has led to nearly every major internet company to pursue CSAM so aggressively that private family photographs are being sent to law enforcement) [perma.cc/T9C8-AXLZ].

23. *See* Nicholas Weaver, *Encryption and Combating Child Exploitation Imagery*, LAWFARE (Oct. 23, 2019) (showing that the technology referred to as hash matching of images is the best way to limit CSAM because it permits a system to assign an alpha-numeric code to an image that allows for passive searches for identical images) [perma.cc/BS7C-NT64].

24. *See* 18 U.S.C. § 2702(b)(6)–(7) (permitting disclosure to either NCMEC or law enforcement).

25. *See* United States v. Jacobsen, 466 U.S. 109, 117–18 (1984) (allowing the government to use information found by a private search because the information is now nonprivate).

enforcement and other government actors to evade the protections promised in the Constitution.[26] The private search doctrine intersects with modern technology when hash matching is both a useful tool for protecting children[27] and a dangerous weapon for governments seeking to repress elements of their society.[28] Allowing government agents to bypass the procedural protections that otherwise exist raises a question about the true boundaries and dangers of police power.

It is not clear where the line should be drawn between protecting children and protecting individual information from government surveillance. Additionally, it is challenging to know how likely the government is to overreach and abuse information gained from this technology. The goal is not to permit free reign for predators, but to ensure that the existence of predators is not being used as an excuse to justify a generally applicable tool being used against the American public at large. This Note will explore and address the issues around the private search doctrine, location data, hash-value matching, and the balance between freedom and safety.

Part II of this Note explores the relevant technologies; Part III outlines the foundations of the Fourth Amendment and the private search doctrine; Part IV explains the existing circuit split on the private search doctrine; Part V discusses the issues surrounding the intersection of technology and the private search doctrine; Part VI explores a variety of solutions to the tension between wanting to avoid surveillance and wanting to stop CSAM; and Part VII concludes.

---

26. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

27. *See Technologies to Stop CSAM: Robust Hashing.*, NETCLEAN (explaining that robust hashing can effectively stop CSAM from being shared because it can review the visual content of images) [perma.cc/26E5-3X5N].

28. *See* Kurt Opsahl, *If You Build it, They Will Come: Apple Has Opened the Backdoor to Increased Surveillance and Censorship Around the World*, ELEC. FRONTIER FOUND. (Aug. 11, 2021) (discussing how hash matching can be used to thwart encryption and censor Chinese citizens) [perma.cc/S6W2-33Q3].

II. Hash Matching: collecting data to gift and sell to the government.

Hash-value matching ("hash matching") is the practice of using an algorithm to generate a short string of characters to represent a larger piece of data, such as a digital image.[29] The algorithm can then passively search an almost limitless amount of data to discover a likely match.[30] This practice is widely utilized by private technology companies to identify criminal material, such as child pornography, and forward it to law enforcement.[31] Major companies are systemically sharing contraband identified using hash matching with various law enforcement and government watch organizations.[32] They avoid becoming government actors themselves despite essentially acting as investigators because a reporting requirement is not viewed as determinative to the analysis, but a search requirement is.[33] So long as the government does not threaten punitive action against a private company for not surveilling their users, the Fourth Amendment cannot be implicated by the private company's actions.[34]

The hash matching process is a sweeping surveillance by private companies that the current criminal justice system relies on in order to identify child sexual abuse material ("CSAM") or those engaging in any other form of child exploitation.[35] However, the practice is also broadly used for copyright infringement,

29. *See* United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016) (summarizing the automated hash matching filter used by American Online).

30. *See id.* (noting that hash matching is used for all images attached to emails that are sent through their servers).

31. *See* Weaver, *supra* note 23 (discussing the current practice of major companies engaging in a campaign of mass surveillance).

32. *See* Roth, *supra* note 22 (explaining that the fear of negative press has led to nearly every major internet company to pursue CSAM so aggressively that private family photographs are being sent to law enforcement).

33. *See* United States v. Rosenow, 33 F.4th 529, 540 (9th Cir. 2022) (noting that federal law leaves private companies free to not search so any search that occurs must be of their own volition).

34. *See id.* at 542 (focusing on Facebook's investigation being volitional).

35. *See* Weaver, *supra* note 23 (arguing that government systems rely on bulk surveillance by private companies).

limiting protest activity, and finding stolen files.[36] As history has shown, aggressive government action is not an absurd notion during political protests.[37] Hash matching can be an essential tool for government action against citizens because it allows for content specific searching through anything touching the internet.[38] Hash matching could very easily be used to track who owns a copy of the Quran, who has authored medical studies that disagree with a government vaccine narrative, or who has access to a document that the government would prefer to remain classified.

III. Foundations of Fourth Amendment Jurisprudence and the Private Search Doctrine.

The Fourth Amendment holds that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[39] This is not a guarantee against all searches and seizures, only those that are unreasonable.[40] The Fourth Amendment generally views any searches and seizures inside of a home as unreasonable absent a warrant.[41] Historically, this type of trespassory standard was the most prominent aspect of the Fourth Amendment.[42] In 2012, the

36. *See* Denae Kassotis, Note, *The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243, 1247 (2019) (noting both the broad applications of hash matching and the tendency of private companies to be encouraged to turn over evidence to law enforcement).

37. *See* Siladitya Ray, *Canada Begins to Release Frozen Bank Accounts of 'Freedom Convoy' Protestors*, FORBES (Feb. 25, 2022) (discussing the freezing of bank accounts to help stop protests against vaccine mandates) [perma.cc/REB8-43FV].

38. *See Digital Safety Content Report*, MICROSOFT (explaining that Microsoft is partnered with numerous government organizations with the goal of using hash-matching technology to actively search users) [perma.cc/VA3V-X8YA].

39. U.S. CONST. amend. IV.

40. *See* Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness.").

41. *See* Payton v. New York, 445 U.S. 573, 586 (1980) ("[S]earches and seizures inside a home without a warrant are presumptively unreasonable.").

42. *See* Olmstead v. United States, 277 U.S. 438, 464–65 (1928) (determining that tapping telephone wires to listen to conversations was not an unreasonable search under the Fourth Amendment because the wires were outside of the home).

Supreme Court found that there is a search within the meaning of the Fourth Amendment when the government trespasses upon a constitutionally protected area "for purposes of obtaining information."[43] This revived the trespassory standard.[44] That is, the protection is implicated by an invasion of a protected private space. The largest alteration in Fourth Amendment jurisprudence occurred when the meaning of the Amendment was considered outside of a Constitutionally protected area.

A. Katz: The Modern Doctrine protecting areas where privacy is expected.

In 1967, the Supreme Court created an important part of the modern Fourth Amendment jurisprudence by developing the reasonable expectation of privacy test.[45] The test is a two-prong examination which considers (1) whether the individual had a subjective expectation of privacy and (2) whether that expectation of privacy is one that society is prepared to recognize as reasonable.[46] The subjective prong is rarely determinative, and even sometimes referred to as the "phantom doctrine" because it is far more challenging for the government to disprove than the objective prong.[47] Courts require the violation of both the subjective and objective expectations of privacy to find that a search occurred, and if a search did occur, then the Fourth Amendment was infringed.[48] This doctrine is used to determine

43. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012) (explaining that a physical intrusion into private property for purposes of gathering information is a search under the Fourth Amendment).

44. *See id.* at 407 (noting that there was no erosion of the principle that invasion violates the Fourth Amendment).

45. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (arguing that the Fourth Amendment protects people and what they work to preserve as private).

46. *See id.* at 361 (Harlan, J., concurring) (presenting the rule determining the protection the Fourth Amendment provides to subjective expectation of privacy).

47. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 133 (2015) ("Although the Supreme Court says that *Katz* is a two-part test, the subjective prong has become a phantom doctrine.").

48. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (applying the Fourth Amendment as a test using two separate questions).

whether a given government action is a search within the meaning of the Fourth Amendment.[49] A search within the meaning of the Fourth Amendment is generally unreasonable absent a warrant in the same way that a trespass would be.[50] The obligation to obtain a warrant is known as the warrant requirement.[51] The warrant requirement holds that a warrantless search is invalid unless an exception applies to the warrant requirement.[52] If a warrantless search occurs without a valid warrant exception, then all evidence obtained by the unconstitutional search is inadmissible in a federal court regardless of its source.[53] This practice of excluding evidence is known as the exclusionary rule.[54] Some examples of warrant exceptions are the good faith exception[55] and the public observation doctrine.[56]

49. *See id.* (explaining that a valid claim requires an invasion by the government).

50. *See* Kentucky v. King, 563 U.S. 452, 459 (2011) (noting that a warrant is required absent an exception).

51. *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (discussing the warrant requirement as a basic principle of the Fourth Amendment).

52. *See id.* (observing that the warrant requirement has exceptions because "the ultimate touchstone of the Fourth Amendment is 'reasonableness'" (quoting Flippo v. West Virginia, 528 U.S. 11, 13 (1999))).

53. *See* Mapp v. Ohio, 367 U.S. 643, 654–55 (1961) (determining that exclusion of improperly obtained evidence is necessary to prevent official lawlessness).

54. *See id.* at 654 (describing the recent consideration of the exclusionary rule).

55. *See* United States v. Leon, 468 U.S. 897, 920–21 (1984) (establishing that when a police officer attempts to act in good faith there is no improper action that the exclusionary rule could deter and so it should not apply).

56. *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (explaining that the public observation doctrine prevents one from having a reasonable expectation of privacy with information that one has revealed to the public).

B. Walter and Jacobsen: the development of the Private Search Doctrine to allow the government to replicate searches by private citizens.

The private search doctrine was created by the Supreme Court in 1980.[57] The case of *Walter v. United States* involved a package of pornographic contraband that was shipped to the wrong address.[58] The Court determined that government actors could warrantlessly examine materials given to the government by a private party so long as the government did not exceed the scope of the private search.[59] The private party looked at some but not all of the tapes with their naked eye.[60] Meanwhile, the government investigators viewed the films contained in the package on a projector, which was considered a significant expansion of the private party's search.[61] The Court decided that when there is a significant expansion of a private party's search, it is considered as a separate search from the private party's search.[62] The Court's reasoning was that a private party's search frustrates the individual's expectation of privacy in part, but does not strip the remaining expectation.[63] This means that law enforcement would need to receive a warrant prior to taking any action that goes beyond the actions of the private party. For example, a private party opened a crate and found that it contained boxes labelled as cocaine. This discovery caused them to contact law enforcement. Law enforcement would be able to open the crate, but they would not be permitted to open the boxes inside of it absent a warrant.

---

57. *See* Walter v. United States, 447 U.S. 649, 657 (1980) (examining the Fourth Amendment in the context of materials arguing that a private search justifies a re-examining of the materials).

58. *Id.* at 652.

59. *See id.* at 657 (comparing scope limitations in official searches to the scope limitations that should logically apply for private searches).

60. *Id.* at 652.

61. *See id.* (describing the actions of the government investigators).

62. *See id.* at 657 (arguing that using a projector to better view the small pictures in the films was a substantial expansion of the search). *But see* State v. Nieves, 999 A.2d 389, 393–94 (N.H. 2010) (noting that an article in plain view has no privacy rights as stated by the plain view exception).

63. *See* Walter v. United States, 447 U.S. 649, 657 (1980) (viewing the expansion of a search as a separate search).

Walter emphasized that if the results of a private search are in plain view when materials are turned over to the government, it may justify the government replicating the prior search before getting a warrant.[64] However, when the government can merely draw inferences about the content of an item following a private search, an act that reveals the nature of that item constitutes a significant expansion of the private search.[65] "[T]he government may not exceed the scope of the private search unless it has the right to make an independent search."[66]

The private search doctrine was examined again in 1984.[67] The case of *United States v. Jacobsen* involved a Federal Express package that was damaged by a forklift.[68] When the shipping company began to inventory the package, bags of white powder were discovered.[69] The company contacted the Drug Enforcement Administration ("DEA"), and placed the discovered contents back into the box prior to the DEA arriving.[70] When the DEA arrived, they opened the box, removed the bags of white powder, and tested the powder for cocaine.[71] The powder tested positive for cocaine.[72]

The *Jacobsen* Court determined that the W*alter* standard meant that additional invasions of privacy by the government must be tested by the degree to which they exceeded the scope of the private search.[73] A government agent viewing "what a private party had freely made available for his inspection" does not violate the Fourth Amendment.[74] Taking actions that enable government

64. *See id.* (allowing that if the results of a private search are readily available, then it may justify the re-examination of the same material).

65. *See id.* (emphasizing that no one could do more than draw inferences about the film's content).

66. *Id.*

67. *See* United States v. Jacobsen, 466 U.S. 109, 122 (1984) (claiming that there is a clear difference between a privacy interest that society is willing to accept and an expectation that something will not be brought to the attention of law enforcement).

68. *Id.* at 111.

69. *Id.*

70. *Id.*

71. *Id.* at 111–12.

72. *Id.* at 112.

73. *See id.* at 115 (explaining the implications of existing precedent).

74. *Id.* at 119.

agents to learn nothing beyond what had previously been uncovered during a private search is permitted.[75] Any government intrusion that exceeds the scope of the private intrusion must be examined independently to determine if it is an unlawful search within the meaning of the Fourth Amendment.[76] The government's actions in this case were found to be permissible.[77] Interestingly, they were found to be permissible despite the government taking part of the drugs and destroying them during a drug testing process.[78] The court rationalized the action by arguing that it did not genuinely invade any privacy because the test could only determine whether the substance was or was not contraband.[79] Further, the destruction of the substance was permitted because the amount taken and destroyed was so small that it could only have a *de minimis* effect.[80]

C. The Private Search Doctrine and when a party is considered a Government Actor.

The private search doctrine draws a clear line between the actions taken by private parties and the actions taken by government actors.[81] Primarily, this occurs because the limitations imposed by the Fourth Amendment only apply to the government.[82] However, it can be challenging to precisely determine who is a government actor for purposes of the private search doctrine. The government actor test utilized by courts is "(1)

75. *See id.* at 120 (emphasizing that the agent's act of removing the bags from the tube was inconsequential).

76. *See id.* at 122 (noting that the field test for cocaine was an additional intrusion).

77. *See id.* at 125 (finding the field test to be reasonable when balancing the law enforcement interest against the private interest).

78. *See id.* at 111–12 (noting that the agent took only a trace amount of the substance for testing).

79. *See id.* at 123 (arguing that a test that merely discloses whether or not a substance is contraband does not compromise any privacy interest).

80. *See id.* at 125 (presenting the seizure as a reasonable action).

81. *See id.* at 119 (analyzing whether the private actions made the government's actions reasonable).

82. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (showing that the Fourth Amendment was designed as a limit on sovereign action).

whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends."[83]

In addition to the issues with the scope of the searches being conducted by private parties, there is an issue with determining when the private companies become government actors. Courts have settled on the test being whether there is a sufficiently close nexus between the government and the challenged action of the private party so that the action can be fairly treated as that of the government.[84] This is relevant around an issue like CSAM because the government is likely to pressure private companies to search for and identify those trafficking in illicit materials. They are likely to do so because there is no way that law enforcement could know who is trafficking in CSAM without a search being conducted by someone. Despite the government actor test, it is unclear when courts will act to disqualify the fruits of private searches, even when government coercion has been prominent.[85]

D. The Private Search Doctrine summarized as a test allowing the fruits of a government search to be admitted so long as the search does not exceed the scope of prior private action.

The private search doctrine can be summarized as a test stating that the fruits of a government search are admissible if that search does not exceed the scope of the prior private search. However, there is inevitable ambiguity for what the scope of the search is and how the scope of the search should be measured.[86] The scope of a physical search is easy to determine because it

83. United States v. Cleveland, 38 F.3d 1092, 1094 (9th Cir. 1994).

84. *See* Jackson v. Metropolitan Edison Co., 419 U.S. 345, 350–51 (1974) (noting that regulation is not sufficient to transform a private party into a government actor).

85. *See* State v. Pauli, 979 N.W.2d 39, 52 (Minn. 2022) (explaining that even if the government had told Dropbox to conduct a search, Dropbox would remain a private actor because they have a business interest in removing CSAM).

86. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554 (2005) (demonstrating the principles behind discovering the scope of a search in a physical search are challenging to apply to a virtual search).

intuitively correlates with what is hidden or exposed.[87] The intuitive understanding of scope is not present for virtual searches. Broadly, there are three possible methods to understanding the scope when it comes to computers and cell phones: the physical box, the virtual file, or the exposed data.[88] The physical box approach means that any access of a computer by a private party should remove privacy interests for the entire computer.[89] The virtual file approach limits the scope to the specific file that was examined by a private party.[90] The exposed data approach considers whether the data was left exposed, meaning that privacy interests remain for any data an individual does not expose regardless of the actions taken by the private party.[91]

When the private search doctrine is applied to a simple container like a box, it is a rather straight forward examination. That is, the government actor can simply recreate the search of the same physical container, and there is little room for confusion in this situation. The various approaches highlight that the situation becomes more complex when computers or cell phones are involved due to the scale of the information that they can contain.[92] For example a private search of a folder containing photographs removes some privacy interest. However, that folder could contain ten or ten thousand photographs. Law enforcement would have no reasonable way of determining which photographs, if any, would require a warrant to review.

87. *See id.* (explaining that physically entering a house is a search and opening a closed container within the house is a separate search).

88. *See id.* at 554 (breaking down the ways of applying search principles to computer data into three basic options).

89. *See id.* at 555 (viewing storage disks as a container).

90. *See id.* at 554 (using an individual file as a unit of measurement).

91. *See id.* at 556 (focusing on the output device as a method of measuring exposure).

92. *See id.* (asking whether a right to look at one file on a server should open the entire server to law enforcement).

IV. The Private Search Doctrine's Circuit Split around determining when government actors can warrantlessly review data provided by private companies.

A. Hash Matching and Big Data surveillance methods for users of the internet.

As previously discussed, hash matching is the practice of using software to convert a piece of data into an alphanumeric string that the software can then compare to its existing store of hash values to find identical pieces of data.[93] This widespread technology is used online for everything from password verification to identifying pirated software.[94] However, the scale of it is rarely recognized. Major companies such as Microsoft, Alphabet, and Meta hash the data that crosses their massive services.[95] This has the potential to implicate social media posts, emails, instant messages, and even documents on a computer that is connected to the internet.[96] These companies explain that their goal is identifying harmful content.[97] The harmful content is what typically reaches courts because it is often some manner of CSAM.[98] The split between circuits involves two different standards to identify exactly when a private search has occurred in a hash matching context.[99] That is, the split is over what needs

93. *See* Kassotis, *supra* note 36, at 1247 ("[L]aw enforcement can compare a suspect's hard-drive against a customized hash-list to look for files stolen during an intrusion.").

94. *See id.* (remarking that private companies hash user data to defend copyrights).

95. *See NCMEC, Google and Image Hashing Technology*, GOOGLE SAFETY CTR. (explaining that private companies actively share hash matching technology and use it to provide information to the government) [perma.cc/79AU-9JVK].

96. *See* Roth, *supra* note 22 (noting that major technology companies are scanning both devices and uploaded images).

97. *See id.* (describing a case of the searches leading to a registered sex offender being arrested).

98. *See generally* United States v. Powell, 925 F.3d 1 (1st Cir. 2018) (discussing Omegle's disclosure of the defendant's child pornography production using the platform).

99. *Compare* United States v. Wilson, 13 F.4th 961, 972 (9th Cir. 2021) (emphasizing the importance of whether a Google employee had viewed the defendant's files before the government's search), *and* United States v. Ackerman,

to occur before a government actor may warrantlessly review the information identified by major technology companies.

B. The Human Actor Standard: requiring a private person to have looked at data before a government actor is allowed to.

The human actor standard is focused on the idea that the private search doctrine should be viewed as a standard analysis of the *Katz* test.[100] It argues that an objective expectation of privacy is lost when a human being views a private item, but no expectation of privacy is lost when something other than a human being sees the same item.[101] This standard requires that a private human being examine a file identified by hash matching for the private search to have occurred.

The Tenth Circuit adopted the human actor standard in 2016.[102] In *United States v. Ackerman*, American Online ("AOL") identified an email as having an attachment with a hash value that matched known child pornography.[103] AOL forwarded this email to NCMEC, a company statutory tasked by the federal government with reviewing hash matched child pornography found by internet service providers.[104] AOL forwarded the email to the government actor without opening the email itself.[105]

---

831 F.3d 1292, 1308 (10th Cir. 2016) (finding that NCMEC conducted a search when it opened the defendant's emails), *with* United States v. Miller, 982 F.3d 412, 428–32 (6th Cir. 2020) (finding that a search did not occur when a detective viewed files already reviewed by a private automated search), *and* United States v. Reddick, 900 F.3d 636 (5th Cir. 2018) ("[D]etective Ilse reviewed only those files whose hash values corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program. So, his review did not sweep in any '(presumptively) private correspondence that could have contained much besides potential contraband.'" (quoting *Ackerman*, 831 F.3d at 1307)).

100. *See Ackerman*, 831 F.3d at 1306–07 (analyzing the facts of the case to determine whether there was information that had remained hidden).

101. *See Wilson*, 13 F.4th at 972 (emphasizing that the government viewing what no other person had seen was central in their analysis).

102. *See Ackerman*, 831 F.3d at 1306 (determining that the scope of the search was exceeded because no private employee had viewed the email in question).

103. *Id.* at 1294.

104. *Id.*

105. *Id.* at 1306.

The Tenth Circuit began by explaining that the corporation receiving alleged child pornography is a government actor.[106] They then identified the private search doctrine test as a two-part inquiry.[107] First, whether the scope of the private search was exceeded.[108] Second, whether the portion of the search that exceeded the private search risked disclosing "information previously unknown to the government besides whether the one attachment contained contraband."[109] Through that inquiry, the court held that opening an attachment that had never been viewed by AOL, exceeded the prior private search.[110] Additionally, the court found that in viewing the message, the government "could have learned all kinds of private and protected facts."[111] This was essential to their consideration of the risk of disclosure.[112] Notably, the court likened emails to virtual containers for purposes of this test and comparing it to *Jacobsen*.[113] The court held that the private search doctrine did not apply.[114]

The Ninth Circuit also adopted the human actor standard in 2021.[115] In *United States v. Wilson*, Google identified four files of child pornography using hash values, and they forwarded this to the police as required by federal law.[116] The report included the photographs as well as the defendant's email address, and several IP addresses.[117] Google did not open or view the files submitted with the report.[118] The police viewed the attachments and used

106. *Id.* at 1295–300.

107. *Id.* at 1305.

108. *See id.* at 1305–06 (beginning with an analysis of whether NCMEC exceeded the private search).

109. *Id.* at 1306.

110. *Id.*

111. *Id.*

112. *See id.* ("[T]hey could have revealed virtually any kind of noncontraband information to the prying eye.").

113. *Id.*

114. *Id.*

115. *See* United States v. Wilson, 13 F.4th 961, 972 (9th Cir. 2021) (determining that the government exceeded the scope of the prior search by opening a file that no Google employee had).

116. *Id.* at 965.

117. *Id.*

118. *Id.*

them to obtain a search warrant for the defendant.[119] The court decided that the government bears the burden of proving that the warrantless search was justified by the private search doctrine.[120]

A key aspect of their holding is that even if the attached files were exact duplicates of the files that Google had used to create their hash values, the private search doctrine would not have applied.[121] Their primary justification was that a private party viewing other digital communications cannot function to validate the private search doctrine.[122] That is, even two identical files are considered separate. The court found that when the government's actions might risk exposing new and protected information, it has exceeded the scope of the prior search.[123]

These two decisions make it clear that the rule is based around human action.[124] This is more of a standard application of the *Katz* test than a distinct rule.[125] It states that a government actor may review something that one has no objective expectation of privacy in, and that one cannot have an objective expectation of privacy in something that a private party has already reviewed.[126] Therefore, a private party must have reviewed the file at issue before a government actor may view it without a warrant.[127] This standard also addressed the issue of determining the scope of the search by

119. *Id.* at 965–66.

120. *See id.* at 971 (arguing that a warrantless search is presumptively unreasonable unless an exception applies).

121. *See id.* at 972 ("[E]ven if they were duplicates, such viewing of others' digital communications would not have violated Wilson's expectation of privacy in his images, as Fourth Amendment rights are personal.").

122. *See id.* at 975 ("Even if Wilson's email attachments were precise duplicates of different files a Google employee had earlier reviewed and categorized as child pornography, . . . we must specifically focus on the extent of Google's private search of *Wilson's* effects . . . .").

123. *See id.* at 971–72 (arguing that by virtue of the government uncovering new information, it exceeded the prior private search).

124. *See* United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016) (focusing on the fact that an AOL employee never opened the email at issue).

125. *See* United States v. Wilson, 13 F.4th 961, 971–72 (9th Cir. 2021) (maintaining a focus on an expectation of privacy being objectively reasonable when no other person had seen the email).

126. *See id.* at 972 (emphasizing that the investigator viewed images that no employee could have).

127. *Id.*

looking exclusively at whether there was a risk of the government encountering any new information.[128]

C. The Virtual Certainty Standard: a private search occurs so long as it is statistically likely that the government actor will discover contraband.

The virtual certainty standard argues that because the algorithm is almost always correct, when an algorithm identifies a file as contraband, it is virtually certain to be contraband.[129] This equates a hash match to a search for purposes of the private search doctrine using a legal fiction where even if a private party has not seen the file the government may warrantlessly review it. That is, this standard does not require any private actor to see anything before the government is allowed to review a personal file.

The Fifth Circuit implemented the virtual certainty standard in 2018.[130] In *United States v. Reddick*, the defendant uploaded digital image files to a Microsoft cloud program that automatically scanned his files for their hash values.[131] The system detected a match with a known image of child pornography, and it automatically sent the files to NCMEC—a government agency.[132] The court held that the government's act of opening the file did not constitute a significant expansion of the private search because the flagged files are almost always correct and the act of opening the file merely confirmed that it was indeed child pornography.[133]

The Sixth Circuit implemented the virtual certainty standard in 2020.[134] In *United States v. Miller*, Google's hash value system

128. *See id.* at 972–73 (demonstrating the substantial amount of new information the government obtained).

129. *See* United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018) (arguing that the file was so likely to contain contraband that opening it merely confirmed that it was the suspected contraband).

130. *See id.* (permitting the viewing of an image to dispel residual doubt caused by no private party actually viewing the images).

131. *Id.* at 637–38.

132. *Id.* at 638.

133. *See id.* at 639 (allowing Microsoft's software to act as the private party inspecting the file).

134. *See* United States v. Miller, 982 F.3d 412, 429 (6th Cir. 2020) (comparing Google's autonomous search of files to an employee inspecting a box).

identified two files as matching hash values for child pornography through an email account.[135] Those files were automatically forwarded to NCMEC without any Google employee reviewing the files, and after review by NCMEC were sent to law enforcement.[136] Along with the files, the police received the IP addresses associated with the account and a profile page for a connected social media website.[137] The police department opened and viewed the files, which confirmed that they showed child pornography.[138] The court then presented an argument regarding whether Google is a government actor, focusing on the fact that no statute compelled the hash value searches.[139] During their analysis, the court assumed that the police violated the defendant's reasonable expectations of privacy and examined the case under the private search doctrine.[140] The court applied a version of the private search doctrine that used a unique test.[141] The test required the private actor's search to, "create a 'virtual certainty' that a government search will disclose nothing more than what the private party has already discovered."[142] Under that test, the court found that *Jacobsen* controls, and that the decision of the court should hinge on whether hash value searches are virtually certain to be correct.[143] This resulted in allowing Google's actions because there was no challenge to the reliability of hash matching which left the court to find that it was virtually certain.[144]

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

139. *See id.* at 423–24 (determining that Google neither performed a public function nor acted under compulsion).

140. *Id.* at 427.

141. *See id.* at 428 (combining multiple case outcomes to develop a test).

142. *Id.*

143. *See id.* (asking whether a digital search could minimize the likelihood of improper discovery to the same degree that a human search would have).

144. *See id.* at 430 (acknowledging that the burden of proof had not been met).

D. The Tension Between Protecting Fourth Amendment Rights and pursuing child predators has shifted the debate towards the optimal way to infringe the Fourth Amendment.

There is clear tension between the interests of the Fourth Amendment and the desire to protect children. On one hand, individuals' Fourth Amendment rights should prevent the government from gaining access to every digital file that one has ever touched. On the other hand, the government's desire to protect children is admirable and expected. Yet, the desire to protect children has shifted the debate from careful balancing to the optimal way of warrantlessly invading an enumerated Constitutional right.

It appears from the cases discussed in the circuit split that while technology may provide great opportunity to society, it presents an active threat to children. In an ideal situation, criminals trafficking in CSAM will be prosecuted without any innocent party having their Fourth Amendment rights impacted. However, that is not a reality. The goal must inevitably be to minimize the ability of criminals to act without shrinking Fourth Amendment protections. Clearly, some courts are so influenced by the potential harm to children that they are willing to create a legal fiction that represents a misinterpretation of Supreme Court precedent.[145] This situation has to be resolved, but the resolution must seek to limit the existing tension between the desire to punish those trafficking in CSAM and the goal of protecting the Fourth Amendment.

The human actor standard clearly provides more protection for individuals than the virtual certainty test, and is correctly focused on the privacy interest being limited by a private party. The virtual certainty standard focuses on the mathematical success with which a given company's hash value system operates.[146] However, the method of obtaining the virtual certainty was actually the essential piece for the *Jacobsen* court that helped

145. *See id.* at 428 (accepting that a computer code can both create near certainty regarding the content of an image and that the certainty created by a digital program has the same privacy impact as a human's eyes).

146. *See id.* at 418 (highlighting the level of accuracy of hash matching).

create the virtual certainty test.[147] *Jacobsen* does not concern itself with the statistical likelihood that a given search uncovered everything of relevance in a specific receptacle.[148] Rather, *Jacobsen* focuses on the fact that a box had already been opened and fully explored by a private party, and that the government's search was only necessary because the private party had returned the items to the box before they arrived.[149] To compare the practice of hash matching to *Jacobsen's* box, the private party would need to open and explore the file in question for it to be analogous to *Jacobsen*. This means that a true interpretation of the language responsible for the creation of the virtual certainty test leads to the human actor standard.

It is of note that the police's opening of a file is not analogous to the taking of the cocaine from the package for testing. A clear bag filled with white powder is not the same as a file on a computer. The contents of a file cannot simply be broken down to be either one thing or another because the scale of information that can be contained in one is so substantial. A photograph is necessarily many things at once.

The private search doctrine caselaw illustrates that a privacy interest can only be infringed by another human being. One is not concerned with their diary being exposed to a tree. The virtual certainty test is flawed because it assumes that a privacy interest can be infringed by a non-sentient party—the algorithm. Comparatively, the human actor standard is a far more reasonable proposition.

The human actor standard, while better than the virtual certainty standard, is still fundamentally inadequate. The human actor standard allows hash matching searches to be used in criminal prosecutions without limit so long as a private party takes

147. *See* United States v. Jacobsen, 466 U.S. 109, 119 (1984) (allowing in person testimony from employees that had physically searched the box to create a virtual certainty about its contents).

148. *See id.* (noting that the re-examination avoided any risk of the employees' recollection).

149. *See id.* (explaining that it was highly likely that a second manual inspection would unveil something the first manual inspection did not).

a few seconds to open the file before sending it.[150] This standard appears to be more in line with a logical view of the Fourth Amendment than the virtual certainty test.[151] Requiring a private party to actually examine a document before law enforcement is consistent with the *Jacobsen* opinion because the Supreme Court was explicitly focused on the fact that the contents had been examined and cataloged prior to law enforcement's search.[152] Extending a human like ability to violate privacy rights to computer algorithms is distinct from extending the ability to violate privacy rights to private individuals. Yet, an employee of a private company viewing a flagged file does not address that fact that the invasion of privacy is occurring.

V. The problems surrounding the Private Search Doctrine.

A. Both Sides of the Circuit Split allow sweeping Searches without Probable Cause because neither side of the split takes issue with surveillance by private companies.

Both sides of the circuit split problematically permit sweeping searches without any finding of probable cause because they do not address the party conducting the search. A key problematic element is that neither side takes issue with the initial surveillance by private companies. Rather, the Fourth Amendment search that initiates the split is the opening of a given file. An action that simply reveals the presence or absence of that which is illegal is not a search under the Fourth Amendment.[153] The key to this consideration is that the opening of a file can reveal

150. *See* United States v. Wilson, 13 F.4th 961, 972 (9th Cir. 2021) (taking issue with the fact that no Google employee could have known or said what the images showed).

151. *See* Payton v. New York, 445 U.S. 573, 588 n.26 (1980) (noting that absent exigent circumstances the strength of a law enforcement officers' belief cannot justify warrantless action).

152. *See Jacobsen*, 466 U.S. at 121 (stating that any privacy interest had been compromised and that the investigators had already learned about the contents directly from the employees).

153. *See* Illinois v. Caballes, 543 U.S. 405, 409 (2005) (distinguishing an individual's expectation that certain facts will not be revealed to police from society's objective expectation of privacy).

far more than just that information. The opened file could be contraband or it could be a confidential legal document. It is the potential for any number of different private facts being revealed that differentiates hash matching from *Jacobsen's* cocaine test.

Neither standard addresses the root issue of private data being examined at an unprecedented scale.[154] Neither standard could function to prevent the existing issue of private companies using hash matching to search data without any limit and then giving that data to law enforcement.[155] In areas outside of hash matching courts have been unwilling to permit such a practice.[156] Admittedly, the primary reason that the private search doctrine has allowed hash matching to be consistently used is almost certainly the nature of the crimes at issue. The cases being considered around the issue of hash matching and the private search doctrine often involve CSAM. It is undeniable that attempting to block any potential tool for finding and destroying CSAM is a morally dubious proposition. However, there is nothing in the language of the doctrine that limits the application of hash matching and the private search doctrine to CSAM. Becoming blinded by the current application of the technology is improper when it could just as easily be used to identify medical tests that cast doubt on a government vaccine or a copyrighted movie. The concern with hash matching and the private search doctrine is not the criminal nature of the content, but that it allows for the very dragnet searches the Fourth Amendment is intended to prevent.[157]

Hash matching can search millions of people at once, and that fact is still problematic even if only a small number of people end

154. *See Wilson*, 13 F.4th at 965 (emphasizing that Google did not review the files before forwarding them to a government actor).

155. *See* Ari Friedman & Matthew McCoy, *Op-Ed: Another Threat to Abortion Privacy? Health Websites Tracking and Sharing your Data*, L.A. TIMES (Dec. 29, 2022) (noting that the average medical clinic website sends personal data to nine different companies) [perma.cc/4BPU-V6YY].

156. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 340–41 (4th Cir. 2021) (barring the use of drone surveillance because it is beyond what law enforcement could do prior to the digital age).

157. *See* United States v. Knotts, 460 U.S. 276, 284 (1983) (suggesting that if a dragnet-style law enforcement practice does develop, then the Supreme Court may act to prevent it in spite of their inaction regarding beeper devices).

up being charged criminally.[158] In *Leaders of a Beautiful Struggle v. Baltimore Police Department*,[159] the court found drone searches encompassing the entire city of Baltimore highly problematic even though the results were deleted except for the small number of data points that law enforcement wanted to review for purposes of bringing criminal charges.[160] The court said, "the preserved 14.2 percent is the needle in the proverbial haystack that the AIR program was designed to discover."[161] The Baltimore surveillance program is highly analogous to hash matching searches because both are broad searches that result in a small number of prosecutions. The heinous nature of a given crime does not excuse or justify a sweeping search even when the search results in only a small number of prosecutions.

Disregarding the sweeping search issue, the limited protection of the human actor standard is open to attack. In *Wilson*, the government provided limited evidence for the accuracy of Google's process.[162] Future courts may rule differently if the record is more developed. Further, even without a future court attempting to circumvent the *Wilson* standard, all that is necessary to avoid implicating the Fourth Amendment is to have the private company review the materials prior to forwarding it to the government. This is true for both the human actor courts and the virtual certainty courts, leading to two important questions: should a private company be able to review the entirety of someone's life using technology, and should the government then be able to use that data? The private search doctrine does not answer those questions adequately. The private search doctrine was developed around

158. *See NCMEC, supra* note 95 (explaining that major companies, such as Microsoft, Alphabet, and Meta, search their entire databases using hash matching).

159. *See Leaders of a Beautiful Struggle*, 2 F.4th at 347–48 (finding that a technology that enables the collection of all movements requires a warrant).

160. *See id.* at 337 (noting that law enforcement kept the fruits of their surveillance program).

161. *Id.*

162. *See* United States v. Wilson, 13 F.4th 961, 972 (9th Cir. 2021) (explaining that the limited record prevented the government from establishing the actions taken by employees and the nature of the images in question).

packages being shipped.[163] It is not a rule built to address a situation where courts must analyze the complexities associated with a mass surveillance technology.[164]

B. The Government Actor test undermines the Fourth Amendment because private companies can be pressured to surveille citizens.

The government has been shown to encourage private action so that they can gather data for prosecution that law enforcement would not be able to get absent a warrant.[165] The encouraging of private action can occur through the government being an avid customer.[166] While that is concerning, it is even more problematic when the encouragement is coercion or inducement. A private actor may feel pressure to ensure that they have a favorable relationship with the government that regulates their business. Two recent cases illustrate the issues that exist within the private search doctrine, and the issues that exist in attempting to navigate the tension between Fourth Amendment rights and the desire to punish those trafficking in CSAM. Both cases demonstrate that government actors can encourage, request, or provide tips to private companies and still benefit from the private search doctrine. They demonstrate law enforcement's existing capacity to skirt the Fourth Amendment.

In *United States v. Rosenow*,[167] the defendant was arrested after returning from the Philippines where he had engaged in sex

163. *See* United States v. Jacobsen, 466 U.S. 109, 111–12 (1984) (describing the routine inspection of a damaged package).

164. *See* Commonwealth v. Almonor, 120 N.E.3d 1183, 1209 (Mass. 2019) (asserting that privacy rights cannot be shrunk by technology and they must be protected as law enforcement adopts and uses new technologies).

165. *See* Jessica Lyons Hardcastle, *Why Bother with Warrants When Cops Can Buy Location Data for Under $10k?*, THE REGISTER (Sept. 1, 2022) (discussing companies that are creating surveillance subscriptions to fill a need created by law enforcement) [perma.cc/S76X-VXHV].

166. *See id.* (describing the large number of law enforcement organizations purchasing subscriptions).

167. *See* United States v. Rosenow, 33 F.4th 529, 534 (9th Cir. 2022) (affirming a conviction despite claims that Yahoo and Facebook were government actors).

tourism with a minor.[168] At issue in the case was whether Yahoo and Facebook were government actors when they searched his devices.[169] Both Facebook and Yahoo have policies to investigate CSAM.[170] Further, the Protect Our Children Act of 2008[171] states that a service provider can face substantial fines if they fail to report apparent violations of the Act.[172]

Yahoo was informed by a money transfer company about the sale of child pornography in the Philippines.[173] They conducted several internal investigations and gave all of the information to the FBI on several occasions due to their understanding that children were being exploited.[174] Meanwhile, the FBI let the investigation lapse from 2015 until 2017, and then they determined that the reports had grown stale.[175] Upon learning that a Facebook account for the defendant existed, the FBI sent preservation requests and administrative subpoenas to Facebook for the defendant.[176] Facebook conducted an investigation into the account and sent tips to the NCMEC as required by the Act. NCMEC gave the information to the FBI who, in turn, used the information to receive a search warrant.[177]

The defendant argued that the private companies were government actors because their searches were all at the behest of the government.[178] In the case of Yahoo, their actions were all

168. *See id.* at 535 (summarizing the event that started the case).

169. *See id.* (noting the claim that both Yahoo and Facebook were government agents during the search).

170. *See id.* at 542 (explaining that Yahoo exercised a contractual right from their terms of service and that Facebook had an internal policy to investigate any CSAM report from law enforcement).

171. 18 U.S.C. § 2258A(a).

172. *Id.* § 2258A(e); *see also Rosenow*, 33 F.4th at 535 (explaining the act's requirement on electronic communication service providers to report apparent violations of criminal offenses involving child pornography).

173. *Id.* at 535.

174. *Id.* at 535–36.

175. *Id.* at 536.

176. *Id.* at 536–37.

177. *Id.* at 537.

178. *See id.* at 539 (arguing on that the private companies were government actors on multiple grounds including that the searches were at the behest of the government).

compelled by federal law.[179] In the case of Facebook, they responded to tips and requests sent by the FBI.[180] Regardless, the court found that the defendant had no reasonable expectation of privacy in his subscriber information or his IP log in information as collected by electronic communication service providers ("ESP").[181]

When examining whether the ESP's were a government agent, this court determined that while a federal law encouraging private searches can transform private action into governmental conduct, that is not the case when the private company is granted substantial enough flexibility to contract the search process to a third party.[182] Further, it emphasized that federal actions cannot transform a private actor when it does not mandate the search.[183] Yahoo's actions did not cross this barrier because the initial discovery was not mandated.[184] Additionally, Facebook's acquiescence to the tip and request did not cross the barrier because it was not technically mandatory for them to do anything.[185]

The court explained that even when a federal statute does not expressly convert private action into government action, the Fourth Amendment can be implicated if there is a close nexus between the government and the private actor.[186] The nexus test is "(1) whether the government knew of and acquiesced in the

179. *See* 18 U.S.C. § 2258A(a) (creating a legal duty to report online sexual exploitation of children).

180. *See* United States v. Rosenow, 33 F.4th 529, 536–37 (9th Cir. 2022) (describing the preservation requests and subpoenas that the FBI sent to Facebook).

181. *See id.* at 548 (distinguishing communication content from user account information).

182. *See id.* at 540–41 (noting that if no statute prevents a service provider from contracting the search process away, then there cannot be enough government participation to violate the Fourth Amendment).

183. *See id.* at 540 (demonstrating that absent a government–mandated search the search must have been desired by the company).

184. *See id.* at 542 (observing the substantial amount of independent action that Yahoo took).

185. *See id.* (finding that while law enforcement knew how Facebook would respond, Facebook's response was still the result of an internal policy to assist law enforcement).

186. *See id.* at 541 (seeking to measure the amount of government involvement in the actions of the private companies).

intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends."[187] The court focused on the fact that Yahoo received a tip from a private company, and so found that government's statutory involvement was insufficient to trigger Fourth Amendment scrutiny.[188] The court found that even the explicit FBI requests to Facebook did not serve as government knowledge or acquiescence under the nexus test because there was already an internal investigation policy for conduct threatening child safety.[189] The court also determined that because there is an independent motivation for the private action, the second prong was not met.[190] The independent motivation was presumably to not have CSAM associated with their company.

Rosenow demonstrates that the Fourth Amendment is not clearly implicated in a case where service providers search for information on their own servers, even at the request of the government. The issue courts will have with using the nexus test is that it opens the door for private companies to argue that they conducted sweeping surveillance for their own benefit. Logically, this is a truthful claim if the company uncovered particularly reprehensible behavior. However, that does not change the fact that the companies have a vested interest in ensuring that they have beneficial relationships with the government.[191] Most importantly, this case not only finds a right to search individual information existing on a private company's servers, but also that a mandate to report is categorically different from a mandated

187. *Id.* (citing United States v. Cleveland, 38 F.3d 1092, 1094 (9th Cir. 1994)).

188. *See id.* at 542 (noting that it is unlikely that law enforcement ever sought Yahoo's help).

189. *See id.* (arguing that Facebook's action was a decision to make corrective action).

190. *See id.* at 544–45 (deciding that a company and the government can share an interest without implicating the Fourth Amendment so long as the independent motive is shown).

191. *See* Edward Ongweso, *Big Tech Has Made Billions Off the 20-Year War on Terror*, VICE (Sept. 9, 2021) (explaining that major technology companies and social media companies have made billions through government contracts over the past two decades) [perma.cc/GF5R-9Z6X].

search.[192] Therefore, this court finds that mandatory reporting statutes cannot implicate the Fourth Amendment.[193] That is true to such a degree that the court found no violation to the defendant's right to privacy.[194]

In *State v. Pauli*, the defendant was charged with possession of child pornography after digital photographs were identified in his online cloud storage account provided by Dropbox.[195] The Dropbox terms of service state that individual data is treated as though it is on a computer's hard drive.[196] It also contained notice that the content could be shared if it violated their terms of service.[197] Logically, these are inconsistent statements unless Dropbox believes that it can search any individual user's hard drives.

The NCMEC received a report through their CyberTipline from an employee of Dropbox.[198] The employee viewed the images that accompanied the report, satisfying the human actor standard.[199] The NCMEC viewed the attached images, determined they contained CSAM, and forwarded them to law enforcement.[200] A law enforcement agent viewed the images, confirmed they contained CSAM, and applied for a search warrant for the defendant's Dropbox account.[201] The defendant moved to suppress the evidence gained from that warrant on Fourth Amendment grounds, but the district court determined there was not an objective expectation of privacy in the images.[202] Additionally, the district court claimed that even if there was an objective expectation of privacy, the private search doctrine permitted the

192. *See* United States v. Rosenow, 33 F.4th 529, 539–41 (9th Cir. 2022) ("Mandated *reporting* is different than mandated *searching*.").

193. *See id.* at 540 (determining that compliance with a reporting statute is insufficient).

194. *See id.* at 548 (finding no violation of privacy from the government subpoenas).

195. State v. Pauli, 979 N.W.2d 39, 43 (Minn. 2022).

196. *Id.* at 44.

197. *Id.* at 43.

198. *Id.* at 44.

199. *Id.*

200. *Id.*

201. *Id.*

202. *Id.* at 45.

law enforcement's warrantless action because they did not expand the initial private search conducted by the Dropbox employee.[203] The defendant appealed the decision, the intermediate appellate court in Minnesota affirmed the decision, and the Supreme Court of Minnesota granted the defendant's request for further review.[204]

A point of issue in the case was whether a tip had been given to Dropbox, but the Supreme Court of Minnesota elected to dismiss the concern.[205] The Supreme Court of Minnesota determined that even if the government had given Dropbox a tip to examine the defendant's account, the private search doctrine was not exceeded because Dropbox has a business interest in keeping CSAM off of its servers.[206] This is a concerning conclusion because it suggests that the government may ask a company to conduct a search, require them under penalty of law to report the results of the search, convict someone using the results, and not violate any portion of the Fourth Amendment. This sweeping surveillance at the behest of the government is analogous to the Baltimore Police Department's decision to maintain prosecution related information from their comprehensive drone program.[207] In that case, law enforcement surveilled the entire city before deleting all data that they were not able to use for criminal prosecution.[208]

Such behavior is concerning on its face because it violates the core of the Fourth Amendment.[209] The Fourth Amendment analysis should not be governed by the method of the invasion, but rather the invasion of privacy regardless of the technology

---

203. *Id.*

204. *Id.* at 45–46.

205. *See id.* at 51–52 (showing that the claim fails regardless of whether the action occurred).

206. *See id.* at 52 (emphasizing the importance of the search being to assist law enforcement rather than the private party).

207. *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 335 (4th Cir. 2021) (addressing the police department's decision to keep only the minimum information needed to prosecute 200 cases).

208. *See id.* at 334–35 (describing the process of drones using advanced camera equipment to cover the entire city of Baltimore).

209. *See* U.S. CONST. amend. IV (stating that people have a fundamental right to be "secure in their persons).

employed.[210] It should not matter whether it is a drone flying overhead or an analyst inspecting a hard drive. The inspection of files on the universal scale that Dropbox engaged in would absolutely violate any person's reasonable expectation of privacy. People should not expect to be the focus of mass surveillance efforts.

The analogy between the drone surveillance from *Leaders* and hash matching can be attacked using a contraband argument. For example, the passage of the Protect Our Children Act has arguably functioned to approve hash matching for CSAM. That Act shows clear Congressional intent to treat the possession of CSAM as illegitimate.[211] This strengthens the analogy between the white substance from *Jacobsen* and CSAM. That is, so long as the hash matches utilized by the government are used solely to determine whether an image is or is not CSAM, then it is permissible in the same way that the drug test in *Jacobsen* was permissible.[212] The binary application of hash matching may appear analogous to a test for drugs rather than a sweeping drone program. Yet, a contraband test is only permissible once the existence of possible contraband has been uncovered and presented to law enforcement. Under *Jacobsen's* logic, hash matching is used far too early. Hash matching is occurring before any criminal activity is suspected in the same way that the drones filmed people in their daily lives before any crimes were suspected to have occurred. As a result, the comparison of hash matching to a binary contraband test fails. The nature of the uncovered criminal act is irrelevant because the search that uncovered it is incompatible with the Fourth Amendment.

---

210. *See* Silverman v. United States, 365 U.S. 505, 513 (1961) (Douglas, J., concurring) (arguing that the focus of the Fourth Amendment is neither trespass law nor the technicalities of electronic equipment).

211. *See* VanDyck v. United States, No. cv-21-00399, 2022 U.S. Dist. LEXIS 226063, at *31–32 (Ariz. Dist. Ct. Dec. 15, 2022) (noting that the Act treats CSAM as illegitimate in a manner similar to the illegitimacy of cocaine for purposes of permitting a test to reveal whether or not something is illegitimate).

212. *See* United States v. Jacobsen, 466 U.S. 109, 124–25 (1984) (permitting a test for cocaine because it did reasonably implicate privacy beyond confirming whether or not the item was contraband).

C. Aside: the similar struggles in the Third-Party Doctrine's Market Actor Reasoning.

Fourth Amendment considerations in the area of technology brush against several other key doctrines. The most relevant other doctrine is the third-party doctrine.[213] This doctrine is a close mirror to the private search doctrine.[214] While the private search doctrine is concerned with information *uncovered* by a third party, the third-party doctrine holds that one cannot have a reasonable expectation of privacy in information voluntarily *conveyed* to a third party.[215] The key to determining if the third-party doctrine applies is whether or not the party gave the information to the third party with the understanding that they would review it.[216] A possible method of addressing concerns that revolve around the private search doctrine is requiring companies to clearly inform users of their practice of examining user data. If companies make sufficient disclosures, it will transition data acquisition from being in the realm of the private search doctrine to the realm of the third-party doctrine. This would be valuable because it would ensure that each user has genuine notice regarding a technology company reviewing their data. Unfortunately, that notice is unlikely to truly solve the problem.

A variety of technology companies track location and other data through cell phones.[217] This process usually requires applications that have the collection systems built in, and by virtue of having installed the application or affirmatively accepting terms

---

213. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.").

214. *Compare Jacobsen*, 466 U.S. at 121 (permitting law enforcement to replicate a search conducted by a private party), *with* Smith v. Maryland, 442 U.S. 735, 744 (1979) (allowing law enforcement to use information that was voluntarily given to a phone company before being given to law enforcement).

215. *See Miller*, 425 U.S. at 443 (noting that there is no constitutional prohibition against the government receiving information from a third party).

216. *See Smith*, 442 U.S. at 744 (determining that the focus of the analysis is whether the private party assumed the risk that the company would reveal the information to law enforcement).

217. *See* Etzioni, *supra* note 16, at 286–87 (explaining that privacy merchants can collect personal information and sell it to the government or other parties without violating any laws).

or settings, a user provides consent.[218] This is objectionable because many users reflexively consent before receiving any genuine notice.[219] Some courts have agreed with the objection to data being collected in this manner.[220] As a result, the fear of passive data collection and the subsequent resale of data could be solved by courts refusing to permit the third-party doctrine to cover the government's use of the data.[221]

One issue that inevitably follows the third-party doctrine is contract law. As stated, the third-party doctrine is specifically concerned with whether or not the individual at issue expected the third party to review their data. As a result, there is a very real concern that a private company could state in their terms of use that they will review user data for set purposes just as Dropbox did in *Pauli*.[222] The contract issue is substantial because it makes it very likely that regardless of new judicial protections, people could still be tricked into giving away their information every time they use a phone or computer. It may become standard practice for one to give their privacy away any time that they use an online service.[223]

The fact that the third-party doctrine allows law enforcement to evade the Fourth Amendment is fundamentally problematic. This doctrine is often associated with location data. Location data can come from a variety of sources, but cell phones are the most

218. *See* Dori H. Rahbar, Note, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment*, 122 COLUM. L. REV. 713, 736–37 (2022) (explaining that voluntary consent for information gathering happens when one turns on their phone or downloads an application).

219. *See id.* at 737 (arguing that the average person does not have notice that their use of a phone will prompt the sale of their personal data).

220. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528–29 (7th Cir. 2018) (refusing to allow the third-party doctrine to permit the collection of smart-meter data from homes).

221. *See* Rahbar, *supra* note 218, at 742 (contending that the government should not be allowed to purchase commercial location data).

222. *See* State v. Pauli, 979 N.W.2d 39, 43 (Minn. 2022) (showing that Dropbox's terms warn that they will disclose information to law enforcement or other parties).

223. *See* Manoush Zomorodi, *Do You Know How Much Private Information You Give Away Every Day?*, TIME (Mar. 29, 2017) (noting that going online is the equivalent of agreeing to inform the police every time you make a new friend) [perma.cc/TZ9A-L3F3].

common source.[224] Eighty-five percent of American adults own a cellphone and ninety percent of the time spent using it involves an application that could be tracking the user.[225] Further, location data can be attached to other items, such as cars, due to their connection with cell phones.[226] These different types of location data have long been used by law enforcement.[227] Yet, the resistance to law enforcement having unrestricted access to such information has proven substantial, if slow.[228] Similar to hash matching, the use of data brokers has functioned to allow law enforcement to access personal data without the burdens of the warrant process.[229] Most commonly, law enforcement simply purchases a service providing the same information that used to be obtained with a warranted search with the obvious benefit of not needing judicial scrutiny.

It is clear that government actors are using multiple methods to skirt the Fourth Amendment. This means that any solution to the problem of government actors encouraging private companies to surveille individuals cannot be solved through anything as simple as forcing a company to admit that they will review user data. However, that does not mean that valid solutions are unobtainable. Several solutions could serve to address the problem without simply moving the issue from the private search doctrine to the third-party doctrine.

---

224. Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, THE MARKUP (Sept. 30, 2021) [perma.cc/N7CG-9PJ6].

225. Jack Flynn, *20 Vital Smartphone Usage Statistics*, ZIPPIA (Oct. 20, 2022) [perma.cc/Q7D5-EGRK].

226. Thomas Brewster, *Cartapping: How Feds Have Spied on Connected Cars for 15 Years*, FORBES (Jan. 15, 2017) [perma.cc/3VHV-55PX].

227. *See id.* (explaining that law enforcement has a long history of using different methods of tracking a vehicle's location and listening to activity inside the vehicle).

228. *See* Carpenter v. United States, 585 U.S. 296, 309–11 (2018) (determining that an "all-encompassing record" of an individual's movements is not consistent with the Fourth Amendment).

229. *See* Cyphers, *supra* note 10 (showing that a number of companies sell data directly to law enforcement).

VI. Proposals: ways to stop the Government from Skirting the Fourth Amendment.

One of the most concerning aspects of attempting to restrict a technology like hash matching is the fear that it serves no purpose other than to defend the most reprehensible of people. However, these proposals are not structured to be a defense of CSAM or an attack on those seeking to prosecute purveyors in such contraband. Rather, it is a preemptive strike focused on the reality that there is no barrier to prevent the largest technology companies in the world from expanding the use of hash matching to things other than CSAM. Those companies have a vested interest in maintaining favorable relationships with governments. Technology companies reasonably seek to both further their own existing government contracts and to ensure that problematic regulation does not destroy their business. The use could quickly become to track or punish those possessing copyrighted movies, divisive medical studies, classified documents, anti-establishment political leanings, banned books, or religious materials like the Quran.

Solving the issue of the government using an existing Fourth Amendment exception to invade the privacy of individuals is not a simple exercise. As is clear from the Supreme Court's treatment of this area, decisively altering the Fourth Amendment has the potential to have severe unintended consequences.[230] However, it is equally problematic to allow dragnet searches to invade the privacies of the individual. The solutions proposed here are intended to be potentially successful adaptations of existing law. The first solution makes no change to the doctrine itself, but draws a distinction between insolated private searches and systemic private searches. In the alternative, the private search doctrine should be limited to the facts of *Walter* and *Jacobsen*. That change will open the issue so that new, modern solutions may be considered. Following this change, I propose three distinct solutions to the existing problem: implement new legislation,

230. *See Carpenter*, 585 U.S. at 315–16 (explaining that the Court's decision is narrowed to not disturb existing doctrines or conventional surveillance techniques); *see also* Northwest Airlines v. Minnesota, 322 U.S. 292, 300 (1944) (deciding that the Court should be cautious in looking to guard against new technologies so that the Court does not "embarrass the future").

prohibit the current system of hash matching searches by private companies through a judicial prohibition, or develop a combined legislative and judicial solution that protects the individual without unduly handicapping law enforcement.

A. Isolated v. Systemic Private Searches.

The issues surrounding the private search doctrine could be addressed by implementing an aspect of the exclusionary rule developed by the Supreme Court to limit systemic problems. The Supreme Court considered in *Herring v. United States*[231] whether the exclusionary rule could apply when officers reasonably, but wrongly, believed that their conduct was backed by a warrant.[232] The Court noted that the exclusionary rule is intended to deter improper conduct by law enforcement.[233] Therefore, law enforcement must have been "sufficiently deliberate" and "culpable" in violating an individual's constitutional rights that the "deterrence is worth the price" of valuable evidence.[234] That is, if the police had violated constitutional rights purely by accident, then no deterrence could occur by applying the exclusionary rule. That reasoning means that isolated negligence does not warrant suppression.[235] Yet, if the problems were systemic, then it might warrant suppression.[236] This echoed the words of Justice Kennedy, "if a widespread pattern of violations were shown . . . there would be reason for grave concern."[237]

The same principle could be applied to the private search doctrine. The original private search doctrine was designed to account for individual activity rather than the systemic activity

231. *See* Herring v. United States, 555 U.S. 135, 147 (2009) (deciding that exclusion is improper when dealing with an error caused by individual negligence rather than systemic error).

232. *See id.* at 137 (explaining that the parties agreed that the action violates the Fourth Amendment).

233. *See id.* at 144 (noting that the rule "serves to deter" improper conduct).

234. *Id.*

235. *See id.* at 137 (determining that the jury should see the evidence because it was only gathered by isolated negligence).

236. *See id.* at 144 (suggesting that the court would view recurring negligence differently).

237. Hudson v. Michigan, 547 U.S. 586, 604 (2006) (Kennedy J., concurring).

caused by hash matching. The private search doctrine is logically appropriate when it ensures that a college student who looks through their roommate's computer and discovers CSAM is able to give it to law enforcement for prosecution. The problems that have been identified in this Note only begin when that private action becomes systematic. That is, when a major organization takes continuous action to search individuals and provide the fruits of those searches to law enforcement. If the principle from *Herring* were applied to the private search doctrine, then an individual discovery would be permissible while a systemic process that resulted in the same discovery would be barred.

It is not a stretch to apply this principle to the private search doctrine because it is highly analogous to the Supreme Court's repudiation of the silver platter doctrine. The silver platter doctrine was a loop-hole in the exclusionary rule that permitted federal law enforcement to receive improperly obtained evidence that had been secured by state authorities and then presented to federal agents on a silver platter.[238] The Supreme Court dispensed with the silver platter doctrine in its entirety.[239] The Court explained that permitting the doctrine would destroy judicial integrity, and that courts should not allow themselves to "be accomplices in the willful disobedience of a Constitution they are sworn to uphold."[240] The private search doctrine is similar to the silver platter doctrine because in both cases law enforcement is receiving information that they could not have permissibly obtained had they taken identical action themselves.

Systemic action against the privacy of the individual is so counter to the principles underlying the Constitution that it is only reasonable to bar the admission of evidence resulting from it. Criticism of searches with no basis in the law is one of the most

238. *See* Lustig v. United States, 338 U.S. 74, 78–79 (1949) (allowing the use of evidence in federal court so long federal agents did not have a hand in gathering it improperly).

239. *See* Elkins v. United States, 364 U.S. 206, 224–25 (1960) ("[E]vidence obtained by state officers during a search which, if conducted by federal officers, would have violated the defendant's immunity from unreasonable searches and seizures under the Fourth Amendment is inadmissible.").

240. *Id.* at 223.

foundational aspects of western legal theory.[241] *Entick* v. *Carrington*, a British case from 1765, presents that very claim.[242] The judge, Lord Camden, argues against searches not clearly authorized by law even in atrocious cases because the power "would be more pernicious to the innocent than useful to the public."[243] The Supreme Court endorsed Lord Camden's statements stating that "[t]he principles laid down in this opinion affect the very essence of constitutional liberty and security."[244] The Court applied these principles not only to all invasions by the government, but to the invasions by the employees of the government into the privacies of life.[245] The Supreme Court also stated, "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property."[246] The Supreme Court's endorsement of *Entick* and condemnation of improper invasion shows that the original state of the constitution argues against permitting systemic invasions to the individual.

The private search doctrine could remain unchanged and still be adapted to modern technology through the application of a more originalist stance. Individual, private action does not present a substantial threat to the Fourth Amendment regardless of the form, but systemic private action does. The private search doctrine can be barred from use when the private search is part of a systemic practice rather than independent action. This adjustment would be consistent with the highly analogous treatment of the silver platter doctrine. It would also not be a radical change. Rather, it would be an example of courts leaning into the originalist principles of the Fourth Amendment and focusing on

241. *See* Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1, 65 (explaining that the earliest Supreme Court decisions applied an exclusionary rule for evidence illegally gathered, and pre-founding statements by judges supported exclusion of evidence).

242. *See Entick* v. *Carrington*, 19 How. St. Tr. 1029, 1045 (1765) (asking whether a minister needs to be given the authority to issue warrants).

243. *Id.* at 1072–73.

244. Boyd v. United States, 116 U.S. 616, 630 (1886).

245. *See id.* (arguing that the rights of liberty held by the Fourth Amendment are broadly applicable).

246. *Id.*

the danger presented by the *invasion* aspect of the private search doctrine.

B. Altering the Doctrine: change the Private Search Doctrine to limit evasion of the Fourth Amendment.

Neither side of the circuit split prevents individuals from having their information closely examined by private companies and then forwarded to government agents to be used against them at the government's leisure. This doctrine was originally created as a physical container rule, and that is a much easier situation to apply it to.[247] That is, if a container is "opened, with its contents laid bare for the world to see, the expectation of privacy in that container has been violated."[248] Yet, the same cannot be said to exist for computers. Computers have the ability to contain such an incredible amount of information that the privacy concerns should be qualitatively different, and so courts should not treat them in the same way as boxes or other physical containers.[249] The Supreme Court aptly noted that it is absurd to compare a wallet to a phone, and in the same way it is absurd to compare a box to a computer.[250]

Due to the lack of individual protection and overall confusion, the doctrine needs to be limited to the facts of the Supreme Court decisions that created it. It needs to be a physical container rule. This not only removes the problematic doctrine from consideration in the technology realm, but it opens the door for a more appropriate solution. The doctrine was created well before the serious privacy concerns created by advanced technology could be

247. *See* United States v. Jacobsen, 466 U.S. 109, 121–22 (1984) (developing the private search doctrine around a physical container that had actually been explored by a private party).

248. Brianna M. Espeland, *Implications of the Private Search Doctrine in a Digital Age: Advocating for Limitations on Warrantless Searches through Adoption of the Virtual File Approach*, 53 IDAHO L. REV. 777, 790 (2017).

249. *See* Dylan Bonfigli, Note, *Get a Warrant: A Bright-line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. CAL. L. REV. 307, 331 (2017) (discussing the implications of the large amount of data stored digitally).

250. *See* Riley v. California, 573 U.S. 373, 391–92 (2014) (describing differing levels of privacy interests based on how substantial the invasion is).

conceived of.[251] The careful balancing of privacy concerns and CSAM warrants new legislation or new legal rules or both. Limiting the private search doctrine provides the opportunity for different solutions to be crafted to solve the existing issue.

C. Enacting Legislative Protections.

A possible solution to the issue is legislation. The Fourth Amendment protects against government action, but hash matching is primarily used by private actors. New legislation can be enacted to stop the invasions by private parties. Other countries have comprehensive privacy protections for individuals.[252] If the United States were to implement similar protections, it may offer a solution that would not require substantial adjustments to judicial interpretations. Statutory protections exist,[253] but other Countries[254] and even one State,[255] have more thorough protections. Certain aspects of these laws can be used to establish new protections against hash matching and similar invasions.

The existing federal protection for individual data in the United States is limited. In 1986, the Stored Communications Act was passed, and it offers the most substantial protection for individuals when it comes to electronically stored data.[256] The Act protects the privacy of the content of communications while they

---

251. *See, e.g.*, Eduardo Medina, *Woman Sues San Francisco Over Arrest Based on DNA From Her Rape Kit*, N.Y. TIMES (Sept. 13, 2022) (describing the case of a woman provided her DNA to police who later used that DNA to charge her for a retail theft) [perma.cc/QD3H-NQK4].

252. *See* Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU (May 25, 2018) (providing a concise summary of the privacy law passed by the European Union) [perma.cc/5D5Q-46GA].

253. *See* 18 U.S.C. § 2702(a) (prohibiting certain disclosures of private data).

254. *See* Commission Regulation, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016/679, 2016 O.J (L 119) 1 (protecting individual's private data and the movement of that data).

255. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199 (2022) (creating several rights designed to protect consumers).

256. *See* § 2702(a) (prohibiting the disclosure of private data by service providers with specific exceptions).

are stored electronically by the service provider.[257] This was clearly designed to work around the limits imposed by the third-party doctrine because it removes those protections for any communications that the user understands the service provider to review.[258] It also has a series of exceptions that prevents the act from limiting the private search doctrine.[259] Specifically, any service provider can reveal the contents of communications that are being sent to NCMEC, are necessary to protect the service provider themselves, were inadvertently obtained and seem to pertain to a crime, are related to an emergency, or are being sent "to any person other than a governmental entity."[260] These exceptions include an immunity from liability for electronic communication service providers so that they can review all user content.[261] The exceptions that are piled onto the existing legislation serve to remove any limitations on either the third-party doctrine or the private search doctrine leaving individuals vulnerable.[262]

Statutory schemes developed by other governments address modern problems more completely. California has enacted the California Consumer Privacy Act of 2018 ("CCPA").[263] A key aspect of the CCPA is the right to know about personal information being collected and used.[264] This style of law could interact with *Katz* to remove objective expectations of privacy and, by virtue of that,

257. *See id.* § 2702(a)(1) (preventing the knowing disclosure of the contents of any communications).

258. *See id.* § 2702(b)(3) (allowing disclosure with consent of either the sender or receiver).

259. *See id.* § 2702(b) (noting the exceptions that permit disclosure of the contents of communications).

260. *Id.* § 2702(b)–(c).

261. *See id.* § 2701(c) (providing enumerated option including for disclosures to the government or NCMEC).

262. *See* Charlie Warzel & Stuart A. Thompson, *How Your Phone Betrays Democracy*, N.Y. TIMES (Dec. 21, 2019) (explaining that a large number of private companies are selling private data to data brokers who resell the data for purposes including voters who lean towards one side of the political spectrum) [perma.cc/SUU9-K5J9].

263. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199 (2022) (creating obligations for private companies that collect personal information).

264. *See id.* § 1798.110 (developing an affirmative right to request disclosure about the information that a company is collecting about the consumer).

place the information obtained by the private party under the third-party doctrine rather than the private search doctrine.[265] This is a clear give and take situation. On one hand, individuals benefit from a formal notice requirement for companies. [266] On the other hand, people are unlikely to internalize how much the notice strips them of privacy protection under the Fourth Amendment.[267] Generally, the CCPA allows customers to identify what data is being collected, the business purpose for it, and lets them request data deletion. California modified the CCPA to expand individual protection for "sensitive personal information" with the California Privacy Rights Act.[268]

The European Union implemented the General Data Protection Regulation ("GDPR") in 2016, and it has been advertised as the "toughest privacy and security law in the world."[269] It implements a series of data protection principles that include ensuring that any data processing is transparent to the data subject, limiting the data processing to only the specific purpose it was gathered for, minimizing the personal data collected to the absolute minimum, and temporally limiting the storage of such data for only as long as is necessary for the purpose gathered.[270] The GDPR also requires that private actors process data only when they have gained the specific consent of the individual, it is necessary to save a life, it is processed to meet a legal obligation, or the private actor has a need to do so in order to perform a task in the public interest.[271] Unfortunately, these seemingly substantial protections do have specific exceptions. Most notably, there are exceptions for both criminal investigations

265. *See* Rahbar, *supra* note 218, at 737 (explaining that consent to data collection alters the legal implications).

266. *See* CAL CIV. CODE §§ 1798.105–1798.115 (creating right to notice, deletion, and to correct inaccurate personal information).

267. *See id.* (allowing companies to maintain information to an unlimited degree so long as they inform the consumer).

268. *See id.* § 1798.100 (requiring collection limitations, notice, and temporal benchmarks).

269. *See* Wolford, *supra* note 252 (summarizing the enacting of the law and the general implications).

270. *See* Commission Regulation, 2016/679, art. 5, 2016 O.J (L 119) 35–36 (listing the principle for managing and processing personal data).

271. *See id.* at 36–37 (requiring only on justification for processing).

and the type of large-scale processing needed to hash match for CSAM.[272] It is clear that the GDPR offers substantial protections to individuals, but still permits practices like hash matching. For example, no specific consent would be needed to examine anything that the government defines as contraband.[273] The legislation is very close to complete so long as the government does not decide that something a citizen wants to view is contraband.

The best practices from the above statutes can be combined and implemented to resolve many of the concerns created by the private search doctrine. The right blend of limitations can end the general practice of government actors encouraging private searches and utilizing the fruits of those searches. The new legislation should have a notice requirement, a deletion of private data right, protection for sensitive information, and strict policies of minimizing data collection. In addition, the legislation must avoid including the numerous exceptions that remove the very protections the legislation proports to establish. There is no point to having privacy legislation if there are exceptions allowing an invasion whenever a private company or the government wishes. If new legislation does offer the listed protections, then the Fourth Amendment should be able to close any other existing gaps.

D. Judicially stop Government Actors from Skirting the Fourth Amendment.

Any legislative solution is dependent on lawmakers, and lawmakers are notoriously slow. Judges can act immediately to stop the existing violation of the principles behind the Fourth Amendment. The Supreme Court has stated that the issue should not be the method of the invasion, but rather the invasion of privacy regardless of the technology employed.[274] The Court has also stated that technology cannot be permitted to erode the

272. *See id.* at 38–39 (permitting the processing of certain categories of personal data and data relating to criminal offenses).

273. *See id.* at 36 ("[P]rocessing is necessary for compliance with a legal obligation to which the controller is subject.").

274. *See* Silverman v. United States, 365 U.S. 505, 512–13 (1961) (Douglas, J., concurring) (contesting the stance that drawing an arbitrary line between types of technology is proper when the degree of the invasion is identical).

privacy guaranteed by the Fourth Amendment.[275] While it may be frustrating to permit the continued existence of contraband, "there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."[276] The principles behind the Fourth Amendment resoundingly state that a desire to prosecute some cannot be allowed to justify the destruction of the Fourth Amendment.[277] The private search doctrine is currently being used to allow sweeping searches with the goal of identifying the few who are trafficking in illicit items.[278] The issue with this is stated best by a dissenting opinion written by Justice Scalia and supported by Justices Ginsburg, Sotomayor, and Kagan.[279] They argue that searching a person for evidence of a crime when there is no basis for believing the person is guilty is prohibited categorically and without exception.[280] While this proposition was stated in a dissenting opinion, any time Scalia and Ginsburg align to condemn a practice, all should stop and listen.

Following these principles, a different solution to the controversy would be for courts to acknowledge that hash matching has no logical limit. It could apply to anything that the ever-fickle legislative branch deems as improper for citizens.[281] When there is tension between a constitutionally enumerated right and a desire to stop an unpleasant behavior the decision must

275. *See* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) (focusing on broad and unsuspecting incursions into privacy).

276. Arizona v. Hicks, 480 U.S. 321, 329 (1987).

277. *See* Gamble v. United States, 587 U.S. 678, 733 (2019) (Ginsburg, J., dissenting) (explaining that the incorporation of the Fourth Amendment blocked the use of improperly obtained evidence by State actors because the identity of the invader was irrelevant from the perspective of the victim).

278. *See* Kassotis, *supra* note 36, at 1247 ("[P]rivate companies are encouraged, both by law and social norms, to turn over evidence of hashmatches to law enforcement.").

279. *See* Maryland v. King, 569 U.S. 435, 466 (2013) (Scalia, J., dissenting) (objecting to the taking of DNA for identification purposes).

280. *See id.* ("Whenever this Court has allowed a suspicionless search, it has insisted upon a justifying motive apart from the investigation of crime.").

281. *See* West Virginia v. EPA, 597 U.S. 697, 739 (2022) (Gorsuch, J., concurring) ("The framers believed that the power to make new laws regulating private conduct was a grave one that could, if not properly checked, pose a serious threat to individual liberty.").

favor the Constitution. As the saying goes, the road to hell is paved with good intentions. A desire to stop the propagation of criminality should not be used to justify violations of the Fourth Amendment. Courts should bar the admission of evidence gathered through warrantless and suspicionless hash matching searches. While this does not stop the invasion by private companies, it could remove the motivation behind it.[282] Most importantly, it ends an existing abuse of the constitution.

E. Develop a joint Legislative and Judicial solution.

While the previous solutions have promise, a proper solution to the complex problems caused by hash matching and the private search doctrine will require both legislative and judicial solutions. This proposal requires Congress to pass legislation that is better than what has already been considered, and for the courts to analyze and limit the effects of that legislation appropriately.

1. Implement the correct legislation.

Congress began considering a comprehensive solution to the CSAM problem in 2020.[283] The EARN IT Act of 2020 conditioned Section 230 liability protections to platforms that follow their commission's best practices.[284] Section 230 prevents defamation suits from being brought against internet companies.[285] Failure to follow the commission's best practices removes Section 230 protections for any service provider.[286] This risked turning the

282. *See* Rahbar, *supra* note 218, at 753 (arguing that it is necessary to treat the government differently than private entities who are untouched by the Fourth Amendment to stop the market of voluntary disclosure from destroying privacy).

283. *See* EARN IT Act, S. 3398, 116th Cong. (2020) (seeking to establish a commission for Online Child Exploitation Prevention).

284. *See id.* (amending immunity to not impair or limit a civil action).

285. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (clarifying that there is federal immunity for service providers against any claim that originates with a third-party user of the service).

286. *See* EARN IT Act, S. 3398, 116th Cong. (2020) (explaining that the reduction in immunity does not apply to a provider that is in compliance with the best practices).

service providers into government actors because Section 230 is arguably essential to operating an internet business.[287] It was feared that courts would view this as mandating searches for purposes of the *Rosenow* nexus test for government actors.[288]

The EARN IT Act of 2022 was Congress's second attempt at legislating in this area.[289] The EARN IT Act of 2022 sought to establish the National Commission on Online CSAM.[290] The agency was designed develop and submit "best practices that providers of interactive computer services may choose to engage in to prevent, reduce, and respond to the online sexual exploitation of children."[291] The agency considered cost, impact on data security and privacy, impact on the ability of law enforcement to investigate and prosecute, and current technology.[292]

It is clear that the drafters became aware of the government actor issue because they altered the requirements placed on private companies.[293] As a result, the new legislation sought only to develop "best practices" that companies *may* choose to utilize.[294] However, these best practices would still likely fail the *Rosenow* nexus test, and it is unclear whether courts would have considered the act to be coercive or merely encouraging.[295] Another key shift

287. *See* Dhiral Patel, Note, *Earning Virtual Responsibility: Raising the Level of Accountability for Interactive Computer Service Providers Due to User-Generated Trafficking*, 55 SUFFOLK U. L. REV. 457, 460 (2022) (noting that the Act could align law enforcement with internet service providers in a way that converts them into government actors engaging in warrantless searches).

288. *See* Adi Robertson, *The EARN IT Act is Back in Congress*, THE VERGE (Feb. 1, 2022) (explaining the condemnations for removing privacy protections for users) [perma.cc/5DQ6-2MMB].

289. *See* EARN IT Act, S. 3538, 117th Cong. (2022) (establishing a commission on Online Child Sexual Exploitation Prevention).

290. *See id.* (composing the commission of nineteen members).

291. *Id.*

292. *See id.* (requiring the consideration to be used in developing the best practices).

293. *Compare* EARN IT Act, S. 3398, 116th Cong. (2020) (requiring affirmative action to maintain Section 230 immunity), *with* EARN IT Act, S. 3538, 117th Cong. (2022) (removing Section 230 immunity only after issues have been reported).

294. *See id.* (applying the limitation of immunity more generally).

295. *See* United States v. Rosenow, 33 F.4th 529, 541 (9th Cir. 2022) (presenting the nexus test as requiring both government knowledge and an intent to assist).

that the new act made was eliminating Section 230 protections for any service provider facing a claim derived from CSAM rather than stripping it upon refusal to implement the "best practices."[296]

The legislation attempts failed in part because both were inconsistent with the Fourth Amendment. However, protective legislation could be implemented where offensive legislation failed. As stated in the previous subpart, protective legislation should establish a notice requirement, a deletion of private data right, protection for sensitive information, and strict policies to minimize data collection. Once the new protections are enacted, there will be an opportunity for courts to establish new rules tailored for modern technology. The legislation cannot be expanded in a way which would permit private searches against individuals for use in criminal prosecutions. As a result, courts will need to consider both new exceptions and new limits.

2. Judicial controls to balance legislation with Fourth Amendment principles.

Courts can establish limits on legislation that balance privacy concerns and the desire to stop criminality. First, courts should balance any new legislative exceptions with a warrant requirement. The warrant requirement should be structured so that a warrant is used prior to searches occurring. This is beneficial in three ways: it provides a limitation on the scale of the searches, it provides a bright-line rule for law enforcement to follow, and it adds a degree of trustworthiness to the entire process. In fact, it is not clear why a warrant requirement has not already been established for private search cases involving CSAM. In the majority of private search doctrine cases there is sufficient evidence for probable cause before any government action has occurred.[297]

---

296. *See* Lisa Macpherson & John Bergmayer, *Is the New EARN IT Act "New Wine in an Old Bottle?" Whatever It Is, We're Not Buying It*, PUB. KNOWLEDGE (Mar. 21, 2022) (noting that federal immunity has never protected an internet provider) [perma.cc/4RA7-B6W4].

297. *See* Thomas W. Nardi, Note, *Virtually Uncertain: The Fourth Amendment and Laptops in United States v. Lichtenberg*, 89 TEMP. L. REV. 781,

Second, courts can include the national security exception from the 2018 case *Carpenter v. United States*.[298] In *Carpenter*, the Supreme Court decided that while historical cell site location data in general was contrary to the Fourth Amendment, the balancing of competing interests around the issue required them to allow the practice for national security concerns.[299] The intrusion was not concerning so long as it was clear that the technology could *only* be utilized for national security.[300] Similarly, the courts can ensure that new protections are not unnecessarily burdensome by permitting existing search capabilities to be warrantlessly used for national security purposes. Such a policy is needed so that foreign militants can be identified. However, the limited application of national security ensures that the exception will not be expanded to pursue ordinary citizens. Together this would balance the loss of privacy for citizens while providing additional protection in all other areas.

VIII. Conclusion.

The use of hash matching to prevent the distribution of CSAM has led to a circuit split that attempts to apply an outdated doctrine to a new technology. Hash matching is a uniquely dangerous technology because it permits surveillance at an unprecedented scale. That surveillance has been permitted under the private search doctrine. However, the various courts that have attempted to bend the private search doctrine to make it apply to hash matching have failed. Their solutions neither solve the problems hash matching is being used to address nor protect the Fourth Amendment. Solving the existing tension between technology and the Fourth Amendment will require substantial action. Courts could leave the existing doctrines in place but

814 (2017) (explaining that obtaining a warrant when private parties have incriminating evidence is usually clear-cut).

298. *See* Carpenter v. United States, 585 U.S. 296, 316 (2018) (narrowing the holding of the case so that it does not consider techniques relating to national security).

299. *See id.* (deciding that cell phone location data is protected by the Fourth Amendment without extending that protection beyond the facts of the case).

300. *See id.* (noting that collection techniques used in foreign affairs is also not considered).

prohibit the systemic actions that allowed for surveillance at an unprecedented scale. Alternatively, the private search doctrine could be limited to its original purpose so that a more appropriate solution can be found. Legislation could be proposed to shore up the gaps that have allowed the private surveillance that is essential of the private search doctrine to prosper. Courts could refuse to permit widespread invasions of privacy. Finally, legislatures and judges could work together to change the paradigm of privacy law. Regardless, something must change. Privacy is supposed to be a right, not a luxury.