DIGITAL DOG SNIFFERS

*Alice Park**

U.S. legislators are taking aim at technology companies for their role in the nation's fentanyl crisis. Members of Congress recently introduced the Cooper Davis Act, which would require electronic communications service providers to report evidence of illicit fentanyl, methamphetamine, and counterfeit drug crimes on their platforms to the Drug Enforcement Administration. For the first time, such companies would be obligated to report suspected criminal activity by their users directly to federal law enforcement. While the Cooper Davis Act is modeled after a federal statute requiring providers to report child sexual abuse material (CSAM), the proposed bill targets a qualitatively different kind of crime—one highly dependent on context. By requiring providers to report directly to the government and by prohibiting deliberate blindness to violations, the Cooper Davis Act would incentivize providers to conduct large-scale automated searches for drug-related activity, raising novel questions about the Fourth Amendment's applicability to mandatory reporting laws for crimes other than CSAM.

This Note examines the implications of extending practical and legal frameworks for regulating CSAM—such as the private search doctrine, which has created a circuit split in online CSAM cases—to other contexts. This Note argues that courts should adopt a narrow interpretation of the private search doctrine, in line with the Second and Ninth Circuits, in cases involving automated searches for criminal activity. This approach would resolve the circuit split in CSAM cases and clarify the doctrine's scope for other kinds of warrantless digital searches.

* J.D. Candidate 2025, Columbia Law School. Many thanks to Professor Daniel Richman for his generous guidance and feedback; Jamie Jenkins, Carolina Herrera, and Shaunak Puri for their suggestions; and Susie Emerson, Matthew Nola, Akesh Shah, and the staff of the *Columbia Law Review* for their editorial assistance. I am especially grateful to my parents, who sacrificed their educational dreams so that I could pursue my own.

INTRODUCTION

Fentanyl poisoning is now the leading cause of death among Americans ages eighteen to forty-five, surpassing traffic accidents, suicide, and COVID-19.[1] Electronic communications and social media have played an outsized role in the ongoing opioid epidemic, leading the Drug Enforcement Administration to take aim at technology companies in recent years.[2] In 2021, the DEA issued a public warning about the growing number of fentanyl-laced counterfeit pills being sold online and blamed social media companies for failing to protect their users.[3] Between May 2022 and May 2023, the DEA conducted more than 1,400 investigations resulting in 3,337 arrests and the seizure of nearly 193 million deadly doses of fentanyl.[4] Over seventy percent of those investigations involved social

---

1. DEA Administrator on Record Fentanyl Overdose Deaths, Get Smart About Drugs, https://www.getsmartaboutdrugs.gov/media/dea-administrator-record-fentanyl-overdose-deaths [https://perma.cc/S3UM-JGM7] (last visited Sept. 11, 2024); Fentanyl by Age: Report, Fams. Against Fentanyl (Dec. 15, 2021), https://www.familiesagainstfentanyl.org/research/byage [https://perma.cc/HP3A-JCMQ].

2. See Kristin Finklea & Lisa N. Sacco, Cong. Rsch. Serv., IN12062, Policing Drug Trafficking on Social Media 1 (2022), https://crsreports.congress.gov/product/pdf/IN/IN12062 [https://perma.cc/WAY8-XW4X]; U.S. Gov't Accountability Off., GAO-22-105101, Trafficking: Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking 11 (2022), https://www.gao.gov/assets/gao-22-105101.pdf [https://perma.cc/4PXM-Y37X]; Marcus A. Bachhuber & Raina M. Merchant, Buying Drugs Online in the Age of Social Media, 107 Am. J. Pub. Health 1858, 1858 (2017). Teenagers and young adults are increasingly turning to social media platforms like Instagram and Snapchat to obtain fentanyl and other synthetic opioids. See, e.g., Robin Buller, Their Kids Died After Buying Drugs on Snapchat. Now the Parents Are Suing, The Guardian (Oct. 18, 2023), https://www.theguardian.com/technology/2023/oct/18/snapchat-sued-overdose-deaths [https://perma.cc/Q5UR-P4TW]; Jan Hoffman, Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar, N.Y. Times (May 19, 2022), https://www.nytimes.com/2022/05/19/health/pills-fentanyl-social-media.html (on file with the *Columbia Law Review*). Drug distributors also use social media to connect with manufacturers and buyers. See Comm'n on Combating Synthetic Opioid Trafficking, Final Report 43–44 (2022), https://www.rand.org/content/dam/rand/pubs/external_publications/EP60000/EP68838/RAND_EP68838.pdf (on file with the *Columbia Law Review*) [hereinafter Commission Report] ("The internet presents unique challenges for drug control in that chemical suppliers in Asia openly advertise synthetic opioids and related chemicals on public platforms, including social media forums and B2B websites.").

3. See Devlin Barrett & Elizabeth Dwoskin, With Overdose Deaths Soaring, DEA Warns About Fentanyl-, Meth-Laced Pills, Wash. Post (Sept. 27, 2021), https://www.washingtonpost.com/national-security/dea-warning-counterfeit-drugs/2021/09/27/448fcb18-1f27-11ec-b3d6-8cdebe60d3e2_story.html (on file with the *Columbia Law Review*); see also Devlin Barrett, Poison Pill: How Fentanyl Killed a 17-Year-Old, Wash. Post (Nov. 30, 2022), https://www.washingtonpost.com/national-security/2022/11/30/fentanyl-fake-pills-social-media/ (on file with the *Columbia Law Review*) (reporting that DEA Administrator Anne Milgram described social media sites like Snapchat as "the superhighway of drugs").

Federal law prohibits the distribution of controlled substances by means of the internet without a valid prescription. See 21 U.S.C. § 829 (2018).

4. Press Release, Drug Enf't Admin., DEA Operation Last Mile Tracks Down Sinaloa and Jalisco Cartel Associates Operating Within the United States (May 5, 2023),

media sites and encrypted communications platforms like Facebook, Instagram, Signal, Snapchat, Telegram, TikTok, WhatsApp, Wickr, and Wire.[5]

But these efforts have been insufficient, according to a bipartisan group of congressmembers, and the fentanyl crisis has worsened as "federal agencies have not had access to the necessary data to intervene."[6] To address the inaccessibility of data held by third parties, Senators Roger Marshall and Jeanne Shaheen introduced in March 2023 the Cooper Davis Act, which would require tech companies to report evidence of illicit fentanyl, methamphetamine, and counterfeit drug crimes occurring on their platforms to the DEA.[7] In July 2024, Representatives Angie Craig and Mariannette Miller-Meeks introduced the Cooper Davis and Devin Norring Act, which mirrors the Senate bill, in the House.[8] The proposed legislation would, for the first time, require electronic communications service providers and remote computing services ("providers"[9]) to report

---

https://www.dea.gov/press-releases/2023/05/05/dea-operation-last-mile-tracks-down-sinaloa-and-jalisco-cartel-associates [https://perma.cc/JW73-7FZ3].

5. Id.

6. See Press Release, Jeanne Shaheen, U.S. Sen. for N.H., Shaheen, Marshall's Bipartisan Bill to Crack Down on Online Drug Sales Through Social Media Clears Key Committee Hurdle (July 13, 2023), https://www.shaheen.senate.gov/shaheen-marshalls-bipartisan-bill-to-crack-down-on-online-drug-sales-through-social-media-clears-key-committee-hurdle [https://perma.cc/6E8H-3Q9E] [hereinafter Shaheen Press Release] (reporting that in a five-month period, the DEA conducted 390 drug-poisoning investigations and found that 129 had direct ties to social media).

7. Cooper Davis Act, S. 1080, 118th Cong. (2023). The bill was first introduced in September 2022 by Senator Roger Marshall and died in committee. See S. 4858, 117th Cong. (2022). In March 2023, Senators Marshall and Jeanne Shaheen reintroduced the bill, with Senators Dick Durbin, Chuck Grassley, Amy Klobuchar, and Todd Young as cosponsors. Press Release, Doc Marshall, U.S. Sen. for Kan., Senator Marshall's Cooper Davis Act Heads to the Senate Floor Following Major Victory out of Committee (July 13, 2023), https://www.marshall.senate.gov/newsroom/press-releases/senator-marshalls-cooper-davis-act-heads-to-the-senate-floor-following-major-victory-out-of-committee/ [https://perma.cc/28QL-9N8H] [hereinafter Marshall Press Release].

8. Cooper Davis and Devin Norring Act, H.R. 8918, 118th Cong. (2024); Press Release, Angie Craig, U.S. Rep. for Minn., Rep. Angie Craig Introduces Bipartisan "Cooper Davis and Devin Norring Act" to Stop Fentanyl Trafficking on Social Media Platforms (July 2, 2024), https://craig.house.gov/media/press-releases/rep-angie-craig-introduces-bipartisan-cooper-davis-and-devin-norring-act-stop [https://perma.cc/46LB-NG2U] [hereinafter Craig Press Release]. Representatives Dan Crenshaw, Don Davis, Jake LaTurner, and Kim Schrier cosponsored the bill. Craig Press Release, supra. The Cooper Davis and Devin Norring Act is named after two teenagers who died of fentanyl poisoning after purchasing counterfeit fentanyl-laced prescription drugs on Snapchat. Id.

This Note refers to the proposed legislation as the Cooper Davis Act and primarily deals with S. 1080, as the Senate bill was introduced first and the laws' contents are largely identical. The only material difference between the two bills for purposes of this Note is an encryption-protection provision in the House bill. See infra note 153.

9. This Note adopts the definition of "provider" in the Cooper Davis Act and 18 U.S.C. § 2258E(6) (2018), which refers to an "electronic communication service provider or remote computing service." Electronic communication service providers give to the public the ability to send or receive wire or electronic communications, id. § 2510(15), and

suspected criminal activity by their users directly to federal law enforcement.[10] The Senate Judiciary Committee approved the Cooper Davis Act in July 2023.[11] The bill expired in January 2025.[12]

Providers use a variety of nonhuman moderation tools to detect content that violates their terms of service, such as drug transactions, spam, hate speech, and child sexual abuse material (CSAM).[13] Federal law requires providers to report evidence of CSAM to the National Center for Missing & Exploited Children (NCMEC), but providers are not statutorily obligated to report any other kind of suspected illegal activity.[14] The Cooper Davis Act is modeled after the federal statute requiring providers to report CSAM: the PROTECT Our Children Act of 2008 (PROTECT Act). Both laws aim to make technology companies play a more proactive role in aiding law enforcement and public safety efforts.[15]

While courts have upheld the constitutionality of providers detecting and reporting CSAM pursuant to the PROTECT Act,[16] the proposed bill targets a qualitatively different kind of crime—one highly dependent on context.[17] This Note argues that by requiring providers to report directly to the government and prohibiting deliberate blindness to violations, the Cooper Davis Act would incentivize providers to conduct large-scale automated searches for drug-related activity, raising novel questions about

---

remote computing services provide to the public computer storage or processing services by means of an electronic communications system, id. § 2711(2).

10. S. 1080 § 2.

11. Marshall Press Release, supra note 7. On September 5, 2023, the bill was amended and placed on the Senate Legislative Calendar. Actions - S.1080 - 118th Congress (2023–2024): Cooper Davis Act, S. 1080, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/1080/all-actions [https://perma.cc/5MGR-Y4UJ].

12. The bill was not voted on by the Senate by the time the 118th Congress ended in January 2025. The House bill also died in committee. Actions - H.R.8918 - 118th Congress (2023–2024): Cooper Davis and Devin Norring Act, H.R. 8918, 118th Cong. (2024), https://www.congress.gov/bill/118th-congress/house-bill/8918/all-actions [https://perma.cc/QF3Z-36EE]. While the Cooper Davis Act was not enacted into law, history suggests the bill's cosponsors may reintroduce it in the new congressional session. See supra note 7. And regardless of whether it is enacted, the issues examined in this Note remain relevant as legislatures continue to grapple with public safety concerns and criminal activity on social media platforms. See infra notes 237–238 and accompanying text.

13. See Hannah Bloch-Wehba, Automation in Moderation, 53 Cornell Int'l L.J. 41, 48–66 (2020) [hereinafter Bloch-Wehba, Automation in Moderation] (tracing the history of providers' automated tools to screen, rank, filter, and block user-generated content).

14. See infra section I.A.1 (describing platforms' reporting obligations). Providers often still collaborate with law enforcement voluntarily. See, e.g., Suzanne Smalley, Senate Bill Crafted With DEA Targets End-to-End Encryption, Requires Online Companies to Report Drug Activity, The Record (July 17, 2023), https://therecord.media/senate-dea-bill-targets-end-to-end-encryption-requires-companies-to-report-drugs [https://perma.cc/S2YN-D8VN] (reporting that many social media sites share data with the police).

15. See infra note 25 and accompanying text.

16. See infra section I.B.

17. See infra section II.A.

the Fourth Amendment's applicability to mandatory reporting laws for non-CSAM crimes.[18]

This Note examines the constitutional problems raised by the Cooper Davis Act and, more broadly, legislation requiring providers to report evidence of illegal activity based on automated computer searches of their users' communications. Part I introduces the proposed bill, its model statute, and Fourth Amendment issues stemming from providers' CSAM reporting requirement, including a circuit split over the private search doctrine's application in online CSAM cases. Part II discusses the differences between automated searches for CSAM and drug-related activity and outlines the novel Fourth Amendment questions raised by the Cooper Davis Act. Part III then explores these issues, concluding that courts would likely treat providers as private parties under the bill. Accordingly, Part III argues that courts should adopt a narrow private search exception to the Fourth Amendment, which best balances users' privacy rights against the government's public safety interests. This approach would also resolve the circuit split in online CSAM cases and provide clear guidance to courts as they confront algorithmic search methods in the future.

I. PROVIDERS' FEDERAL REPORTING REQUIREMENTS, FROM CSAM TO FENTANYL

This Part introduces the Cooper Davis Act and the Fourth Amendment issues that its statutory inspiration, the PROTECT Act, has raised. Section I.A describes providers' reporting requirements under the proposed bill and the PROTECT Act. Section I.B then explains how courts have rejected Fourth Amendment challenges to the PROTECT Act scheme under the private search doctrine. Finally, section I.C discusses a circuit split regarding the scope of the private search exception in online CSAM cases.

A. *Comparing the Cooper Davis Act and the PROTECT Act*

1. *The Cooper Davis Act's Reporting Requirements for Drug Crimes.* — The Cooper Davis Act requires providers to report to the DEA "as soon as reasonably possible after obtaining actual knowledge of any facts or circumstances" establishing the unlawful sale, distribution, or manufacture of fentanyl, methamphetamine, and counterfeit substances.[19] Providers are not required to search for illegal drug activity under the bill, and they need not "engage in additional verification or investigation to

18. See infra section II.B.2.

19. Cooper Davis Act, S. 1080, 118th Cong. § 2(a) (2023) (adding § 521(b) to Part E of the Controlled Substances Act, Pub. L. No. 91-513, 84 Stat. 1236 (1970) (codified as amended at 28 U.S.C. § 801 et seq. (2018))). The proposed bill also authorizes, but does not require, providers to submit reports based upon a "reasonable belief" of violations. Id.

discover facts and circumstances that are not readily apparent."[20] But a provider may not "deliberately blind itself" to readily apparent violations of the statute.[21]

Reports to the DEA must include "information relating to the account involved in the commission of a crime."[22] While providers are not required to include the contents of users' electronic communications when reporting information about an account, the Cooper Davis Act authorizes them to report such communications, including "direct messages, relating to [proscribed] activity."[23] The bill also requires providers to specify whether the facts being reported were discovered through content moderation conducted by a human or via "a non-human method" like an algorithm or machine learning.[24]

2. *The PROTECT Act: The Cooper Davis Act's Statutory Inspiration.* — A review of the statutory framework that inspired the Cooper Davis Act helps illuminate the Fourth Amendment issues raised by the proposed bill.[25] Congress enacted the PROTECT Act in 2008 to "increase the ability of law enforcement agencies to investigate and prosecute child predators."[26] The law requires providers to report "any facts or circumstances from which there is an apparent violation of" specified criminal offenses involving CSAM.[27] Providers must submit reports to the National Center for Missing & Exploited Children, a private nonprofit established by Congress in 1984 that operates a centralized reporting system for online CSAM called the CyberTipline.[28]

---

20. Id. (adding § 521(g) to Part E of the Controlled Substances Act); see also infra note 44 (quoting the text of the proposed provision).

21. S. 1080 § 2(a) (adding § 521(g)(4)).

22. Id. (adding § 521(c)(1)(A)).

23. Id. (adding § 521(c)(2)(C)).

24. Id. (adding § 521(b)(1)(C)).

25. See Shaheen Press Release, supra note 6 ("Social media companies . . . have similar reporting requirements for child sexual exploitation under [the] PROTECT our Children Act of 2008. The Cooper Davis Act would establish a comprehensive and standardized reporting regime that would enable the DEA to better identify and dismantle international criminal networks and save American lives."). In a Senate Judiciary Committee hearing, Senator Alex Padilla noted that the CSAM reporting requirement under § 2258A "is what inspired the structure of the bill before us." Sen. Alex Padilla, Sen. Alex Padilla | Padilla Defends Privacy Concerns in Cooper Davis Act | SJC | 7.13.21, YouTube, at 1:15 (July 13, 2023), https://www.youtube.com/watch?v=imYTY0HKG2A (on file with the *Columbia Law Review*) [hereinafter Padilla Remarks].

26. Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (codified in relevant part at 18 U.S.C. § 2258A (2018)).

27. 18 U.S.C. § 2258A(a)(2)(A).

28. Id. § 2258A(a)(1)(B); Missing Children's Assistance Act, Pub L. No. 98-473, 98 Stat. 2125 (1984) (codified as amended at 34 U.S.C. § 11292 (2018)) (authorizing federal funding for the establishment and operation of a national clearinghouse dedicated to improvement in managing cases of missing and exploited children and establishing NCMEC's five mandated functions); CyberTipline, Nat'l Ctr. for Missing & Exploited Child.,

Although CSAM remains ubiquitous on the internet,[29] the CyberTipline has played an instrumental role in curbing the proliferation of CSAM online.[30] In 2023, the CyberTipline received more than 36 million reports of suspected online CSAM, which contained more than 105 million images and videos.[31] Nearly all of those reports came from the tech industry: Five providers—Facebook, Instagram, Google, WhatsApp, and Snapchat—accounted for more than ninety percent of all reports.[32]

Providers typically detect CSAM using hashing technology. Hashing is a forensic technique that takes a large amount of data, like an image or video, and applies "a complex mathematical algorithm to generate a relatively compact numerical identifier" that is unique to that data.[33] This identifier, a hash value, is "a sort of digital fingerprint" for the file.[34] Providers search for CSAM by computing hash values for files uploaded or transmitted by users and automatically comparing those hashes to lists of hashes of known CSAM, a process called hash matching.[35] The most

---

https://www.missingkids.org/gethelpnow/cybertipline [https://perma.cc/5VQN-SA99] (last visited Sept. 10, 2024).

29. See Fernando Alfonso III, The Pandemic Is Causing an Exponential Rise in the Online Exploitation of Children, Experts Say, CNN (May 25, 2020), https://www.cnn.com/2020/05/25/us/child-abuse-online-coronavirus-pandemic-parents-investigations-trnd/index.html [https://perma.cc/458C-JBY3].

30. See MaryJane Gurriell, Born Into Porn but Rescued by Thorn: The Demand for Tech Companies to Scan and Search for Child Sexual Abuse Images, 59 Fam. Ct. Rev. 840, 841–45 (2021).

31. Off. of Juv. Just. & Delinq. Prevention, Off. of Just. Programs, DOJ, CY 2023 Report to the Committees on Appropriations National Center for Missing and Exploited Children (NCMEC) Transparency 4–5 (2023), https://www.missingkids.org/content/dam/missingkids/pdfs/OJJDP-NCMEC-Transparency-CY-2023-Report.pdf [https://perma.cc/24S6-CQGV] [hereinafter OJJDP Report].

32. Nat'l Ctr. for Missing & Exploited Child., 2023 CyberTipline Report 6 (2023), https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf [https://perma.cc/8KDR-FEHL] [hereinafter 2023 CyberTipline Report]; Nat'l Ctr. for Missing & Exploited Child., 2023 CyberTipline Reports by Electronic Service Providers (ESP) 1–8 (2023), https://www.missingkids.org/content/dam/missingkids/pdfs/2023-reports-by-esp.pdf [https://perma.cc/8F8X-XR72]. In 2023, NCMEC escalated 63,892 reports involving children in imminent danger to state and federal law enforcement. 2023 CyberTipline Report, supra, at 3.

33. Richard P. Salgado, Reply, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. Forum 38, 38 (2005).

34. United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016) (citing Salgado, supra note 33, at 38–40); see also PhotoDNA, Microsoft, https://www.microsoft.com/en-us/photodna [https://perma.cc/U79W-XA6C] (last visited Sept. 13, 2024).

35. For instance, Google automatically computes the hash values of all email attachments that its users send or receive. See Michelle DeLaune, NCMEC, Google and Image Hashing Technology, Google Safety Centre, https://safety.google/intl/en_uk/stories/hash-matching-to-help-ncmec/ [https://perma.cc/WM75-7XRC] (last visited Sept. 13, 2024). PhotoDNA, a hash-matching tool developed by Microsoft to detect CSAM, is deployed worldwide across a number of platforms including Facebook, Twitter, and Google. Hany Farid, An Overview of Perceptual Hashing, J. Online Tr. & Safety, Oct. 2021, at 1, 12; see also United States v. Reddick, 900 F.3d 636, 637–38 (5th Cir. 2018)

common hashing technique in CSAM detection is "hard hashing," which requires two files to have the exact same hash value to be considered a match; even a small change in an image or video, like a minor crop or filter, can cause a significant change in the resulting hash.[36] NCMEC maintains a database of nearly eight million hashes of known CSAM files, which dozens of providers use for hash matching, and NCMEC's hash-sharing initiative uses a hard-hashing algorithm.[37]

Some providers also use perceptual image (or "fuzzy") hashing algorithms, which are more resilient to minor alterations like cropping, compression, and color changes.[38] Fuzzy hashing aims to extract "a concise, distinct, perceptually meaningful signature" from an image's pixels and can detect files that have been changed to evade hard-hashing algorithms but are still fundamentally the same content.[39] Microsoft's widely used PhotoDNA tool, for example, uses fuzzy hashing.[40]

When a provider identifies a hash match to known CSAM, it is statutorily obligated to report those files, along with the user's information, to NCMEC.[41] According to the Cooper Davis Act's cosponsors, the bill mirrors providers' reporting requirement under the PROTECT Act by requiring providers to report evidence of drug crimes.[42] Both laws require providers to report when they have "actual knowledge" of the proscribed activity.[43] They also use nearly identical language disclaiming a mandate on providers to proactively search for illegal activity.[44]

(describing the use of PhotoDNA to scan hash values of user-uploaded files and compare them against images in the NCMEC database). In 2014, Google developed its own technology, CSAI Match, to detect known CSAM videos on its services; Google's API is used by NGOs and companies like Reddit, Yahoo, and Adobe. Fighting Child Sexual Abuse Online, Google, https://protectingchildren.google/#tools-to-fight-csam [https://perma.cc/494L-BMND] [hereinafter Google Tools] (last visited Sept. 13, 2024).

36. See Farid, supra note 35, at 4.

37. OJJDP Report, supra note 31, at 11–13 (describing how providers may opt into NCMEC's hash-sharing initiatives); see also Farid, supra note 35, at 3 (citing the MD5 hard-hashing algorithm employed by NCMEC).

38. See Farid, supra note 35, at 3, 5 (explaining "perceptual hashing," also known as "fuzzy hashing").

39. Id.

40. See id. at 12; supra notes 34–36. Meta and Apple also use perceptual hashing algorithms. Tim Bernard, The Present and Future of Detecting Child Sexual Abuse Material on Social Media, Unitary (Oct. 16, 2023), https://www.unitary.ai/articles/the-present-and-future-of-detecting-child-sexual-abuse-material-on-social-media [https://perma.cc/P6CH-5L6M].

41. See 18 U.S.C. § 2258A(a) (2018).

42. See supra note 25 and accompanying text.

43. See supra note 19 and accompanying text; see also 18 U.S.C. § 2258A(a).

44. The PROTECT Act states:

> Nothing in this section shall be construed to require a provider to—
>
> (1) monitor any user, subscriber, or customer of that provider;
>
> (2) monitor the content of any communication of any person described in paragraph (1); or

B. *Mandatory Reporting, Not Mandatory Searching: How Online CSAM Reporting Complies With the Fourth Amendment*

In criminal prosecutions, the government may not use evidence obtained in violation of the Constitution, and, as with any governmental search and seizure, the government's use of information obtained under the PROTECT Act to prosecute criminal defendants is limited by the Fourth Amendment.[45] The Fourth Amendment confers protection onto what a person "seeks to preserve as private, even in an area accessible to the public."[46] When a purported search does not involve physical trespass onto private property, courts apply a two-part inquiry to determine whether a search has occurred: (1) whether a person "exhibited an actual (subjective) expectation of privacy" and (2) whether that expectation is, objectively, "one that society is prepared to recognize as 'reasonable.'"[47] Courts have long held that people have a reasonable expectation of privacy in the contents of their private communications, like letters and telephone calls.[48]

Since its passage in 2008, the PROTECT Act has prompted much litigation and debate over the constitutionality of CSAM detection and

---

(3) affirmatively seek facts or circumstances described in sections (a) and (b).

18 U.S.C. § 2258A(f)(1)–(3).

The Cooper Davis Act states:

> Nothing in this section shall be construed to—
>
> (1) require a provider to monitor any user, subscriber, or customer of that provider;
>
> (2) require a provider to monitor the content of any communication of any person described in paragraph (1);
>
> (3) require a provider to affirmatively search, screen, or scan for facts or circumstances described in subsection (b)(2) . . . .

S. 1080, 118th Cong. § 2 (2023) (adding § 521(g)(1)–(3) to Part E of the Controlled Substances Act).

45. U.S. Const. amend. IV (guaranteeing "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"); Mapp v. Ohio, 367 U.S. 643, 654–57 (1961) (holding that evidence obtained in violation of the Fourth Amendment is inadmissible in court).

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

47. This test originates from Justice John Marshall Harlan's concurrence in *Katz*. See id. at 361 (Harlan, J., concurring). The *Katz* expectation-of-privacy test "has been *added to*, not *substituted for*, the common-law trespassory test." United States v. Jones, 565 U.S. 400, 409 (2012).

48. See *Katz*, 389 U.S. at 352 (holding that individuals have a right to privacy in the contents of their telephone calls). In contrast, there is no reasonable expectation of privacy in *noncontent*, such as phone numbers and to/from email addresses. Ex parte Jackson, 96 U.S. 727, 733 (1877) (holding that the contents of "[l]etters and sealed packages . . . in the mail" receive the same constitutional protection as papers in one's own domicile); see also Smith v. Maryland, 442 U.S. 735, 744 (1979) (phone numbers); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (to/from addresses of emails).

mandatory reporting.[49] But, as this section explains, courts have rejected Fourth Amendment challenges to the government's use of CSAM evidence reported pursuant to the PROTECT Act—even though that evidence implicates the contents of users' private communications—under the private search doctrine.

1. *The Fourth Amendment's State Action Requirement.* — The Fourth Amendment applies only to state action, and its probable cause and warrant requirements do not apply to searches effected by private parties acting on their own initiative, no matter how arbitrary or unreasonable the search.[50] The private search doctrine is an exception to the Fourth Amendment's warrant requirement and allows the government to use information that a private party has voluntarily turned over based on its own search.[51] The government may not, however, "exceed the scope of the private search" unless it has the authority to make its own lawful, independent search.[52]

As the following subsection explains, the Courts of Appeals universally consider providers to be private parties under the PROTECT Act. Accordingly, providers may search for CSAM without implicating the Fourth Amendment, and, under the private search doctrine, the government may warrantlessly use CSAM evidence detected by providers (and then mandatorily reported to NCMEC), so long as it does not "exceed the scope" of the provider's private search.[53]

2. *Providers as Private Searchers.* — A private party is subject to the Fourth Amendment only if it acts as an agent or instrument of the

---

49. See infra notes 59–66, 73–75 and accompanying text (citing CSAM cases in the lower courts); infra section I.C (describing a circuit split).

50. See Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 613–14 (1989) (holding that the Fourth Amendment guarantees "the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction"); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("[The Fourth Amendment's] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority . . . .").

51. United States v. Jacobsen, 466 U.S. 109, 115 (1984) ("Whether those invasions were accidental or deliberate, . . . reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character. The additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." (footnote omitted)).

52. Walter v. United States, 447 U.S. 649, 657 (1980).

53. *Jacobsen*, 466 U.S. at 116; United States v. Maher, 120 F.4th 297, 312 (2d Cir. 2024) (stating that "the private search doctrine is properly understood to authorize law enforcement authorities to conduct a warrantless search only when they repeat a search already conducted by a private party to the same degree it 'frustrate[s]' a person's expectation of privacy" (alteration in original) (quoting *Jacobsen*, 466 U.S. at 117)); United States v. Powell, 925 F.3d 1, 5 (1st Cir. 2018) (holding that the government does not violate the Fourth Amendment so long as its search is "coextensive with the scope of the private actor's private search and there is 'a virtual certainty that nothing else of significance' could be revealed by the governmental search" (quoting *Jacobsen*, 466 U.S. at 119)).

government.[54] Determining whether a private entity is acting as a government agent or instrument is a fact-intensive inquiry that depends "on the degree of the Government's participation in the private party's activities."[55] In *Skinner v. Railway Labor Executives' Ass'n*, the Supreme Court held that federal regulations requiring railroad companies to test some employees for illicit drugs and giving them discretion to test other employees converted the private railroads into government agents for purposes of the Fourth Amendment.[56] The Supreme Court provided only high-level principles in *Skinner* for determining when a private party becomes a government agent, so lower federal courts have formulated their own fact-dependent tests. The most popular Court of Appeals test considers two "critical factors": (1) the government's knowledge of and acquiescence in the search and (2) the intent of the searching party.[57] Some circuits have also drawn from the Supreme Court's state action jurisprudence under the Fourteenth Amendment to determine questions of Fourth Amendment government agency.[58]

---

54. *Jacobsen*, 466 U.S. at 113 (holding that the Fourth Amendment is "wholly inapplicable" to searches conducted by private individuals not acting as government agents).

55. *Skinner*, 489 U.S. at 614.

56. See id.

57. United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981) (first stating the "critical factors"). The Third, Fourth, Fifth, Sixth, Seventh, Eighth, Tenth, and Eleventh Circuits have applied a variation of the "critical factors" inquiry. See United States v. Kramer, 75 F.4th 339, 343 (3d Cir. 2023); United States v. Johnlouis, 44 F.4th 331, 337 (5th Cir. 2022); United States v. Koerber, 10 F.4th 1083, 1114 (10th Cir. 2021); United States v. Bebris, 4 F.4th 551, 561 (7th Cir. 2021) (emphasizing, however, that "no rigid formula has been articulated in this circuit"); United States v. Perez, 844 F. App'x 113, 116 (11th Cir. 2021) (considering "whether the government 'openly encouraged or cooperated in the search'" as an additional factor (quoting United States v. Ford, 765 F.2d 1088, 1090 (11th Cir. 1985))); United States v. Ringland, 966 F.3d 731, 735 (8th Cir. 2020) (considering an additional third factor, "whether the citizen acted at the government's request" (internal quotation marks omitted) (quoting United States v. Wiest, 596 F.3d 906, 910 (8th Cir. 2010))); United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010); United States v. Bowers, 594 F.3d 522, 526 (6th Cir. 2010).

The First Circuit uses a different test that considers: (1) the extent of the government's role in initiating or participating in the search; (2) the government's intent and the degree of control it exercises over the search and the private party; and (3) the extent to which the private party aims primarily to help the government or to serve its own interests. See United States v. Rivera-Morales, 961 F.3d 1, 8 (1st Cir. 2020). The D.C. Circuit has not developed a government agency test. See In re Search of: Encrypted Data Provided by the Nat'l Ctr. for Missing & Exploited Child. for Nineteen Related Cyber Tipline Reps., No. 20-sw-321 (ZMF), 2021 WL 2100997, at *5 n.5 (D.D.C. May 22, 2021) [hereinafter *In re Search of: Encrypted Data*].

58. For example, in holding that Google did not act as a government agent by searching for CSAM, the Sixth Circuit considered three "tests" that the Supreme Court has used to discern state action under the Fourteenth Amendment: (1) a "function" test that asks whether a private party performs a public function; (2) a "compulsion" test that asks whether the government compelled a private party's actions; and (3) a "nexus" test that asks whether a private party cooperated closely with the government. United States v. Miller, 982

Regardless of which test they applied, all circuits to address the question have held that the PROTECT Act does not convert regulated entities into government agents—while federal law requires them to report CSAM, providers remain private parties because the law imposes no duty to "affirmatively search, screen, or scan for" CSAM.[59] As the Ninth Circuit held, "Mandated *reporting* is different than mandated *searching*. . . . [A] private actor does not become a government agent simply by complying with a mandatory reporting statute."[60]

3. *The Question of NCMEC.* — While courts universally treat providers as private parties under the PROTECT Act, they have diverged on whether NCMEC is a government agent. In 2016, the Tenth Circuit became the first and only Court of Appeals to hold that NCMEC qualifies as a governmental entity or agent under the PROTECT Act, emphasizing NCMEC's "special law enforcement duties and powers" established by Congress.[61] Applying the "critical factors," then-Judge Neil Gorsuch held that the PROTECT

F.3d 412, 422 (6th Cir. 2020); see also United States v. Sykes, 65 F.4th 867, 876–77 (6th Cir. 2023) (applying the three tests to Facebook).

The Second Circuit has also applied the nexus test, noting that private actions are attributable to the government "only where 'there is a sufficiently close nexus between the State and the challenged action of the . . . entity so that the action of the latter may be fairly treated as that of the State itself.'" United States v. DiTomasso, 932 F.3d 58, 67–68 (2d Cir. 2019) (alteration in original) (quoting United States v. Stein, 541 F.3d 130, 146 (2d Cir. 2008)).

59. 18 U.S.C. § 2258A(f)(3) (2018); see also, e.g., United States v. Bohannon, No. 21-10270, 2023 WL 5607541, at *2 (9th Cir. Aug. 30, 2023) (holding that Microsoft is not a government agent); *Sykes*, 65 F.4th at 876–77 (same for Facebook); United States v. Rosenow, 50 F.4th 715, 735 (9th Cir. 2022) (Yahoo and Facebook); United States v. Meals, 21 F.4th 903, 907 (5th Cir. 2021) (Facebook); *Bebris*, 4 F.4th at 562 (Facebook); *Ringland*, 966 F.3d at 736 (Google); United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013) (AOL); United States v. Cameron, 699 F.3d 621, 636–38 (1st Cir. 2012) (Yahoo); *Richardson*, 607 F.3d at 364–67 (AOL); *In re Search of: Encrypted Data*, 2021 WL 2100997, at *5 (Google).

The remaining Courts of Appeals have not directly addressed whether providers are government agents, but district court decisions in those circuits are consistent with the general rule. See, e.g., United States v. Tennant, No. 5:23-cr-79, 2023 WL 6978405, at *12 (N.D.N.Y. Oct. 10, 2023) (holding that Snapchat, Instagram, and Discord are not government agents); United States v. Clark, No. 22-cr-40031-TC, 2023 WL 3543380, at *11 (D. Kan. May 18, 2023) (same for Omegle); United States v. Williamson, No. 8:21-cr-355-WFJ-CPT, 2023 WL 4056324, at *13 (M.D. Fla. Feb. 10, 2023) (Yahoo); United States v. Hart, No. 3:CR-20-197, 2021 WL 2412950, at *8 (M.D. Pa. June 14, 2021) (Kik); United States v. Coyne, 387 F. Supp. 3d 387, 396 (D. Vt. 2018) (Microsoft, Oath, and Chatstep).

60. *Rosenow*, 50 F.4th at 730. Numerous circuits have recognized "that a company which automatically scans electronic communications on its platform does 'not become a government agent merely because it had a mutual interest in eradicating child pornography from its platform.'" *Bebris*, 4 F.4th at 562 (quoting *Ringland*, 966 F.3d at 736).

61. See United States v. Ackerman, 831 F.3d 1292, 1295–1304 (10th Cir. 2016). The court emphasized that: (1) NCMEC alone is statutorily obligated to maintain an electronic reporting system and forward reports to federal law enforcement; (2) providers are obligated to report to NCMEC alone; (3) NCMEC is obligated to treat any report it receives as a preservation request issued by the government itself; and (4) NCMEC has a statutory exemption permitting it to receive CSAM knowingly and review it intentionally, which would otherwise subject one to criminal prosecution. See id.

Act's comprehensive scheme reflected congressional knowledge of and acquiescence in NCMEC's actions, and NCMEC possessed the requisite intent to assist law enforcement.[62] No other Court of Appeals has directly addressed NCMEC's status, having avoided the question by resolving Fourth Amendment issues under the private search doctrine; that is, even assuming NCMEC is a government agent, that assumption is usually immaterial since the government may lawfully duplicate searches conducted by private actors, and courts rarely hold that NCMEC exceeded the scope of a provider's private search.[63]

C. *When Does the Government Exceed the Scope of a Provider's Search?*

In a handful of cases, the Courts of Appeals have issued differing rules as to what it means to exceed the scope of a provider's search. Given the near-perfect accuracy of hash matching,[64] providers sometimes submit reports to NCMEC based solely on a hash match without first opening the detected file to confirm it is CSAM.[65] In such cases, courts confront the question of whether the government (or NCMEC, assuming it is an agent of the government) exceeds the scope of the private search by viewing the file.[66] This section discusses two approaches to this question, which has generated a circuit split. The first, the "sui generis" approach taken by the Fifth and Sixth Circuits, argues that the government does not conduct a new search by opening files that matched known CSAM hashes but were

---

62. Id. The court noted that *Skinner* further bolstered its conclusion, as the government exhibited "encouragement, endorsement, and participation," which was enough to render the railroad a government agent. Id. at 1302 (internal quotation marks omitted) (quoting Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615–16 (1989)).

63. See, e.g., *Sykes*, 65 F.4th at 876 (holding that even if NCMEC is a governmental entity, Facebook's private search was not attributable to the government); *Meals*, 21 F.4th at 908 (assuming arguendo that NCMEC was a government agent, it did not exceed the scope of the private search); *Ringland*, 966 F.3d at 736–37 ("[W]e need not decide whether NCMEC is a government agency . . . ."). The Ninth Circuit is the only other Court of Appeals to come close to ruling that NCMEC is a government agent. See *Rosenow*, 50 F.4th at 729–30 n.3 ("There is good reason to think that the NCMEC is, on the face of its authorizing statutes, a governmental entity . . . ."); cf. *Coyne*, 387 F. Supp. 3d at 397 (district court holding that NCMEC is a governmental agent).

64. See infra note 129 and accompanying text.

65. See infra notes 66–80 and accompanying text.

66. In the situation where a human reviewer confirms that a file that triggered a hash match is CSAM before reporting it to NCMEC, courts agree that the government (or NCMEC, acting as a government agent) may warrantlessly view the file without exceeding the scope of the private search, as that would merely replicate the provider's search. See, e.g., United States v. Powell, 925 F.3d 1, 6 (1st Cir. 2018) (holding that, assuming NCMEC was a government agent, it did not expand the scope of Omegle's private search by viewing the exact same files); United States v. Drivdahl, No. CR 13-18-H-DLC, 2014 WL 896734, at *4 (D. Mont. Mar. 6, 2014) (concluding that "there was no expansion of the private search" because the "suspect material was opened by a Google employee prior to being turned over to the government").

not viewed by a private party.[67] Under the second approach, taken by the Second and Ninth Circuits, the government may not warrantlessly take the "first look" at files, even those reported based on a hash match.[68]

1. *The Sui Generis Approach.* — In *United States v. Reddick*, the Fifth Circuit held that law enforcement could use CSAM evidence detected by a provider through hash matching that had not been viewed by any private party.[69] Microsoft's PhotoDNA hashing program identified files that the defendant had uploaded to his personal cloud storage, and Microsoft automatically reported the matches to NCMEC, which then forwarded the report to police.[70] The Fifth Circuit held that a police detective did not exceed the scope of Microsoft's search by opening and viewing the files, analogizing the detective's visual review of the files to the government's actions in *United States v. Jacobsen*, one of the Supreme Court's foundational private search doctrine cases.[71]

In *Jacobsen*, FedEx employees opened a damaged package and found plastic bags containing white powder concealed in a tube.[72] The employees turned over the package to DEA agents, who visually inspected the bags and conducted chemical field tests on the white powder; the tests revealed that the powder was cocaine.[73] The Supreme Court held that the DEA agents did *not* exceed the private search since their tests merely confirmed whether the substance was cocaine—similar to "sniff tests" by narcotics detection dogs, which are not Fourth Amendment searches.[74] The Fifth Circuit emphasized in *Reddick* that, like the chemical tests, the detective's

---

67. Some have used the term "sui generis" in this context to invoke the binary search doctrine and analogize hash searches to dog sniffs. See, e.g., Tyler O'Connell, Comment, Two Models of the Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material, 53 U. Pac. L. Rev. 293, 317 (2021) (describing hash searches as "sui generis" binary searches). But this Note uses "sui generis" to describe a broader reasoning that includes binary search arguments but relies more generally on the certainty with which the government knows a file contains CSAM after a hash match.

68. The Second Circuit has described the "challenging question" raised in the circuit split as

> whether the private search doctrine authorizes law enforcement authorities to conduct a warrantless visual examination of the contents of a digital file where a private party has not visually examined the contents of *that* file but, rather, has used a computer to match the hash value of the contents of that file to the hash value of an image previously located in another file, which image, upon visual examination, was determined to depict child pornography.

United States v. Maher, 120 F.4th 297, 314 (2d Cir. 2024).

69. 900 F.3d 636, 639 (5th Cir. 2018).

70. Id.

71. Id. at 639 (citing United States v. Jacobsen, 466 U.S. 109 (1984)).

72. 466 U.S. at 111.

73. Id. at 111–12.

74. Id. at 123–26 (citing United States v. Place, 462 U.S. 696, 699 (1983)).

review "merely confirmed" that the file was CSAM as the hash match suggested.[75]

The Sixth Circuit has also adopted the sui generis approach.[76] In *United States v. Miller*, the Sixth Circuit held that a police detective did not exceed the scope of Google's private search when he opened email attachments whose hashes were flagged as matching hashes in Google's CSAM database.[77] The court's analysis turned on the "virtual certainty" with which law enforcement knew the files were CSAM before even opening them.[78] Google had already frustrated the user's privacy interest in their files through its hash match, so the detective's actions did not disclose anything more than what Google's search had already shown.[79] In a case also involving Google, a magistrate judge on the United States District Court for the District of Columbia emphasized that before any file is added to Google's CSAM hash database, a Google employee trained in the federal definition of CSAM visually confirms that it is CSAM.[80] As such, while a Google employee may not review every flagged hash match before it is reported to NCMEC, "[t]he chances of Google's submission based on a hash match not being child pornography is 'astronomically small.'"[81]

2. *The First-Look Approach.* — Under the second, "first-look" approach, a provider's hash match does not extinguish a user's privacy interest in their files. In *United States v. Wilson*, the Ninth Circuit created a circuit split by departing from the Sixth Circuit in a case also involving Google, with nearly identical facts as *Miller*.[82] The Ninth Circuit held that law enforcement exceeded the scope of Google's hash search because it (1) learned new, critical information that it then used to obtain a warrant and prosecute the defendant and (2) viewed files that no Google employee or other person had viewed.[83] The court likened the detective's review to

---

75. 900 F.3d at 639.

76. See United States v. Miller, 982 F.3d 412, 418 (6th Cir. 2020).

77. Id. at 417. While *Miller* involved nearly identical facts as *Reddick*, the Sixth Circuit declined to adopt the Fifth Circuit's analogy to the chemical tests in *Jacobsen*. Id. at 429.

78. Id. at 417 (internal quotation marks omitted) (quoting *Jacobsen*, 466 U.S. at 119).

79. Id. at 429–30.

80. *In re Search of: Encrypted Data*, 2021 WL 2100997, at *6.

81. Id. (quoting Salgado, supra note 33, at 39). Some district courts and state supreme courts have also adopted approaches akin to the sui generis approach. See, e.g., United States v. Rosenschein, No. 16-4571, 2020 WL 6680657, at *12 (D.N.M. Nov. 12, 2020) (analogizing the government's opening of previously unseen images to the chemical tests in *Jacobsen*); State v. Lizotte, 197 A.3d 362, 370 (Vt. 2018) (concluding that NCMEC and law enforcement did not exceed AOL's search by opening a video identified through hashing since they already knew from the hash match what the attachment contained).

82. *Wilson*, 13 F.4th 961, 976 (9th Cir. 2021) ("In so holding, we contribute to a growing tension in the circuits about the application of the private search doctrine to the detection of child pornography.").

83. Id. at 971–72.

the government's actions in *Walter v. United States*, the Supreme Court's other major private search doctrine case.[84]

In *Walter*, a package of obscene films was mistakenly delivered to a private company, and an employee opened the package and saw that the film boxes had labels on their exterior indicating they contained obscene pictures.[85] Employees tried and failed to view one of the films by holding it up to the light before turning the films over to the FBI.[86] Without seeking a warrant, FBI agents then viewed the films using a projector.[87] The Supreme Court concluded that the FBI agents' viewing exceeded the employees' search.[88] Even though the agents had acted on probable cause,[89] the warrantless screening was a "significant expansion" of the private search since prior to screening the films, one could only draw inferences about what they contained.[90] In *Wilson*, the Ninth Circuit compared the detective's visual review of the files matching CSAM hashes to the FBI agents' projection of the films in *Walter*.[91] By opening the files, the detective learned exactly what the image showed and whether the image was in fact CSAM, gaining more information than what the hash match alone conveyed.[92]

In October 2024, the Second Circuit joined the Ninth Circuit in ruling that "the private search doctrine does not permit police to conduct

---

84. Id. at 973; see also Walter v. United States, 447 U.S. 649 (1980).

85. *Walter*, 447 U.S. at 651 (plurality opinion).

86. Id. at 651–52.

87. Id. at 652.

88. Id. at 654.

89. The Court noted that the FBI agents had probable cause to believe that the films were obscene based on their labels and that their reason for viewing the films was to determine whether their owner was guilty of a federal offense (interstate shipment of obscene content). Id.

90. Id. at 657.

91. United States v. Wilson, 13 F.4th 961, 973 (9th Cir. 2021).

92. Id. at 973–74. The *Wilson* court also noted that the Tenth Circuit invoked reasoning "consistent" with its approach in *Ackerman*, though the Tenth Circuit did not address this particular question. Id. at 977 (discussing United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016)). In *Ackerman*, AOL's hashing technology had identified one of four images attached to the defendant's email as CSAM, and AOL reported the email's text and all four attachments to NCMEC. 831 F.3d at 1294 (Gorsuch, J.). A NCMEC analyst opened the defendant's email attachments and confirmed that all four—not just the one AOL's hashing algorithm had identified—contained CSAM. Id. After holding that NCMEC was a state actor or agent, then-Judge Gorsuch concluded that NCMEC had exceeded the scope of AOL's search by viewing the three other images. Id. at 1294–308.

While *Ackerman* involved different facts from *Reddick*, *Miller*, and *Wilson*—the information the government viewed for the first time had not been identified by a hash match—the court's reasoning cast doubt on the sui generis approach. Id. The court noted that if the government had viewed only the one image AOL had identified as a hash match, that might have brought it "closer to a successful invocation of the private search doctrine." Id. at 1306–08. But, the court cautioned, such action may still have exceeded the private search since the government could "expos[e] new and protected information"—perhaps if the hash match had been "mistaken." Id. at 1306–07.

a warrantless visual examination of a digital file that a private party has not itself viewed but only computer hash matched to the contents of another digital file previously determined to contain child pornography."[93] That case, *United States v. Maher*, also presented nearly identical facts as *Miller* and *Wilson*.[94] The Second Circuit observed that after a Google employee or contractor identifies material on the platform as CSAM, the company does not retain the image once it has added its hash value to the company's repository.[95] As a result, the Second Circuit emphasized, Google "cannot, based only on a hash match, describe the specific contents of either matched file, *i.e.*, it cannot describe the age of any child depicted, the number of children depicted, whether any adults are also depicted, or the particular circumstances depicted that might be deemed child pornography."[96] Since Google does not convey such specific information to NCMEC, and NCMEC in turn does not convey it to law enforcement, police would be able to obtain that information only by exceeding the scope of Google's hash search and conducting a visual examination of the file.[97]

The Second Circuit understood Google's hash matching technology as having "*labeled* the [defendant's] file image as 'apparent child pornography' much as the pictures and images on the film labels in *Walter*" indicated that the films contained pornographic content.[98] While such a label may provide probable cause to support a warrant to search the containers' contents, "such a search is certainly going to reveal more than the label itself."[99] The Second Circuit thereby rejected the Fifth and Sixth Circuits' reasoning, emphasizing that the police's warrantless visual examination of the file's contents "did not simply replicate Google's own algorithmic search . . . but expanded on it in a way not employed by

93. United States v. Maher, 120 F.4th 297, 318 (2d Cir. 2024) (citing *Wilson*, 13 F.4th at 961).

94. The defendant had uploaded a file to his Google email account, and Google's hash algorithm determined that the file contained an image whose hash value matched a hash in Google's repository. Id. at 303. Google reported the file to NCMEC's CyberTipline, noting in its report that "while the contents of the [reported] file were not reviewed concurrently to making the report, historically a person had reviewed a file whose hash (or digital fingerprint) matched the hash of the reported image and determined it contained apparent child pornography." Id. (alteration in original) (citation omitted) (internal quotation marks omitted). NCMEC, too, did not visually examine the contents of the file, and it sent Google's report and the unopened file to New York police, who viewed the file without obtaining a search warrant. Id. at 303–04. Based on an affidavit describing the contents of this file, police then obtained warrants to search Maher's email accounts and his residence. Id. at 304.

95. Id. at 301 n.2, 303.

96. Id. at 303.

97. See id. at 306.

98. Id. at 318 (citation omitted).

99. Id.

Google, *i.e.*, human visual inspection, which allowed the police to learn more than Google had learned."[100]

Importantly, the circumstances giving rise to this circuit split rarely occur since providers must report to NCMEC, not directly to the government, and NCMEC analysts often view reported files before referring them to law enforcement, thereby extinguishing any privacy interest in those files.[101] Since NCMEC is generally understood to be a private actor that may "exceed" the scope of a provider's search—no matter how one defines that scope—the government may warrantlessly view those reported files under the private search doctrine.[102] Accordingly, the Supreme Court has declined to take up this circuit split in recent years.[103]

---

100. Id. at 306. The Second Circuit explained that it was unpersuaded by the Fifth Circuit's reasoning in *Reddick* because it "d[id] not understand the Fourth Amendment to permit law enforcement officials to conduct warrantless searches of unopened property to confirm a private party's report—however strong—that the property contains contraband." Id. at 315. The court further rejected the Fifth Circuit's analogy to the chemical tests in *Jacobsen* because the Supreme Court did not approve of those tests under the private search doctrine but rather because the tests' "further intrusion was limited to a binary disclosure." Id. (citing United States v. Jacobsen, 466 U.S. 109, 122 (1984)). Likewise, the court rejected the Sixth Circuit's reasoning in *Miller* based on the reliability of hash matching and its analogy to *Jacobsen*. See id. While the DEA agents in *Jacobsen* conducted a warrantless search of the *same* container already privately searched by FedEx employees, "[b]y contrast, in *Miller* and [*Maher*], police conducted a warrantless visual search of a digital file . . . that no Google employee or contractor had ever opened or visually examined. Rather, what a Google employee or contractor had earlier opened and visually examined was a *different* file . . . ." Id. at 317. Accordingly, "[e]ven assuming the high reliability of Google's hash matching technology, it could reveal only that two images are virtually certain to be identical. It could not—and here did not—reveal what in particular was depicted in the identical images." Id. at 318.

101. See id. at 303 (describing how "in many cases . . . Google 'automatically reports' the computer matched image to the NCMEC as 'apparent child pornography' without any person viewing it" (citations omitted)); see also 2023 CyberTipline Report, supra note 32, at 4–8 (noting that NCMEC escalates a tiny fraction of reports to law enforcement).

102. *Ackerman* is the only circuit court decision to hold that NCMEC is not a private party. See supra notes 61–63 and accompanying text.

103. See United States v. Miller, 982 F.3d 412 (6th Cir. 2020), cert. denied, 141 S. Ct. 2797 (2021) (mem.); United States v. Ringland, 966 F.3d 731 (8th Cir. 2020), cert. denied, 141 S. Ct. 2797 (2021) (mem.); United States v. Reddick, 900 F.3d 636 (5th Cir. 2018), cert. denied, 139 S. Ct. 1617 (2019) (mem.). The Second Circuit's recent ruling could revive attention on the issue, but the Supreme Court has been reluctant to take Fourth Amendment cases in recent years, according to some commentators. See, e.g., Orin Kerr (@OrinKerr), X (June 18, 2023), https://x.com/OrinKerr/status/1670467183690784768 [https://perma.cc/7W6P-P2JB] (noting that the Supreme Court granted certiorari on no Fourth Amendment cases in OT2021 and OT2022).

Law students have also proposed solutions to the circuit split that broadly track these two approaches. Compare Kyle Brantley, Comment, The Algorithm's Alright: Trusting Big Tech's Image Match in the Wake of *Wilson*, 58 Wake Forest L. Rev. 525, 546 (2023) (arguing that the Supreme Court should resolve the circuit split by adopting the Fifth and Sixth Circuits' approach), with Virginia Kendall, Note, Constitutional Law—The Current System for Abolishing Child Pornography Online Is Ineffective: The Alternative Measure for

II. AN OLD FRAMEWORK FOR A NEW PROBLEM?

The PROTECT Act dramatically expanded the government's capacity to prosecute CSAM, and the Cooper Davis Act aims to achieve a similar result for fentanyl distribution and other drug crimes.[104] This Part explores the practical and constitutional differences between the two laws. Section II.A examines the differences between how providers search for CSAM and drug crimes. Section II.B introduces the Fourth Amendment issues raised by the Cooper Davis Act and discusses how they relate to the issues courts have faced in CSAM cases.

A. *Automated Technologies to Detect CSAM vs. Drug Crimes*

Many platforms already employ machine learning and artificial intelligence to detect drug-related content on their sites, driven in part by public pressure over the opioid epidemic,[105] and it is plausible that the Cooper Davis Act's passage would prompt further investment into developing technologies to proactively detect drug crimes.[106] While providers detect both drug-related activity and CSAM using nonhuman content moderation, CSAM is uniquely identifiable, through hash matching, with a level of precision and accuracy that has not been

---

Eradicating Online Predators, 45 U. Ark. Little Rock L. Rev. 751, 778 (2023) (offering an approach similar to the Second and Ninth Circuits' rule).

104. See supra note 25.

105. See, e.g., Rachel Lerman & Gerrit De Vynck, Snapchat, TikTok, Instagram Face Pressure to Stop Illegal Drug Sales as Overdose Deaths Soar, Wash. Post (Sept. 28, 2021), https://www.washingtonpost.com/technology/2021/09/28/tiktok-snapchat-fentanyl/ (on file with the *Columbia Law Review*).

106. Snap reported taking action on over 241,000 drug-related accounts in the U.S. from July 1 to December 31, 2023. Transparency Report, Snap Priv., Safety & Pol'y Hub (Apr. 25, 2024), https://values.snap.com/privacy/transparency [https://perma.cc/4XDB-DGVG]. Snap detects eighty-eight percent of drug-related content proactively using machine learning and AI, and when it finds drug-dealing activity, Snap bans the account and blocks the user from creating new accounts; in some cases, it refers the account to law enforcement for investigation. Expanding Our Work to Combat the Fentanyl Epidemic, Snap Priv., Safety & Pol'y Hub (Jan. 18, 2022), https://values.snap.com/news/expanding-our-work-to-combat-the-fentanyl-epidemic [https://perma.cc/WEV3-ZVHD]. In 2022, Meta reported taking action on over fifteen million drug-related exchanges on Facebook and nine million exchanges on Instagram, based on both alerts from users and preemptive detection. Guy Rosen, Community Standards Enforcement Report, Fourth Quarter 2021, Meta (Mar. 1, 2022), https://about.fb.com/news/2022/03/community-standards-enforcement-report-q4-2021/ [https://perma.cc/95KK-QMEY] (describing Facebook's improved and expanded "proactive detection technologies").

The "proactive rate"—the percentage of content identified using machine detection technology—was over ninety-seven percent for Facebook and Instagram. Proactive Rate, Meta, https://transparency.fb.com/policies/improving/proactive-rate-metric/ [https://perma.cc/LQ4K-H8K6] (last updated Feb. 22, 2023); Restricted Goods and Services: Drugs and Firearms, Meta, https://transparency.meta.com/reports/community-standards-enforcement/regulated-goods/facebook/ [https://perma.cc/MX3U-Q7B8] (last visited Sept. 13, 2024).

replicated in any other context.[107] When providers have attempted to proactively detect visual content using automated methods other than hashing, the results have been less than ideal—Facebook and Tumblr, for example, have struggled to accurately detect nudity and sexual content.[108]

Detection of *speech*-based content is an even thornier problem.[109] Language is much more difficult to police on a mass scale given the

---

107. Some providers use hash matching to detect terrorist content on their sites. Facebook, Microsoft, Twitter, and YouTube founded the Global Internet Forum to Counter Terrorism (GIFCT) in response to pressure by European governments to remove terrorist and violent extremist content from their sites following the 2015 and 2016 terrorist attacks in Paris and Brussels, respectively. See About, Glob. Internet F. to Counter Terrorism, https://gifct.org/about/ [https://perma.cc/NNC3-7JP9] (last visited Sept. 13, 2024); Svea Windwehr & Jillian C. York, One Database to Rule Them All: The Invisible Content Cartel that Undermines the Freedom of Expression Online, Elec. Frontier Found. (Aug. 27, 2020), https://www.eff.org/deeplinks/2020/08/one-database-rule-them-all-invisible-content-cartel-undermines-freedom-1 [https://perma.cc/JGH4-YESE].

The GIFCT operates a hash-sharing database containing hashes for terrorist content. GIFCT's Hash-Sharing Database, Glob. Internet F. to Counter Terrorism, https://gifct.org/hsdb/ [https://perma.cc/E82J-HKAY] (last visited Sept. 13, 2024). But efforts to detect terrorist content using GIFCT's hash database have had limited success because terrorist content may be acceptable in certain contexts, such as news reporting, but not in others. See Daphne Keller, Internet Platforms: Observations on Speech, Danger, and Money 7 (Hoover Inst. Aegis Paper Series No. 1807, 2018), https://www.hoover.org/sites/default/files/research/docs/keller_webreadypdf_final.pdf [https://perma.cc/7CHM-JXHH] ("An ISIS video looks the same, whether used in recruiting or in news reporting."). "Countless examples have proven that it is . . . impossible for algorithms[] to consistently get the nuances of activism, counter-speech, and extremist content itself right. The result is that many instances of legitimate speech are falsely categorized as terrorist content and removed from social media platforms." Windwehr & York, supra. The hash database may therefore have a "disproportionately negative effect on news organizations, human rights defenders, and dissidents who seek to expose and comment on violence." Bloch-Wehba, Automation in Moderation, supra note 13, at 76.

108. See, e.g., Paige Leskin, A Year After Tumblr's Porn Ban, Some Users Are Still Struggling to Rebuild Their Communities and Sense of Belonging, Insider (Dec. 20, 2019), https://www.businessinsider.com/tumblr-porn-ban-nsfw-flagged-reactions-fandom-art-erotica-communities-2019-8 (on file with the *Columbia Law Review*) (explaining how Tumblr's use of machine-learning algorithms to flag NSFW media mistakenly flagged pictures of breakfast, anime, and memes as pornography). In 2020, Facebook proactively removed a garden center's ad for onion seeds on the basis that an image of onions was "sexually suggestive." Isobel Asher Hamilton, Facebook's Nudity-Spotting AI Mistook a Photo of Some Onions for 'Sexually Suggestive' Content, Insider (Oct. 9, 2020), https://www.businessinsider.com/facebook-mistakes-onions-for-sexualised-content-2020-10 (on file with the *Columbia Law Review*); see also Denmark: Facebook Blocks *Little Mermaid* Over 'Bare Skin', BBC (Jan. 4, 2016), https://www.bbc.com/news/blogs-news-from-elsewhere-35221329 [https://perma.cc/XND3-8MZ7].

109. Crucially, hash matching is unable to detect illegal activity that necessarily involves speech, like drug transactions. As Senator Padilla explained in a Senate Judiciary Committee hearing on the bill:

> When it comes to discussions of controlled and counterfeit substances, context is pretty important. Drawing the line between someone seriously expressing a desire to acquire meth . . . versus innocent content, such as

importance of context, and automated detection of online hate speech has become an active area of research in the machine learning world, in large part because of how complicated the problem is.[110] Detection of hate speech is difficult to automate because slurs and derogatory language may be hateful only in certain contexts, and certain slurs may be used in ways that do not count as hate speech.[111] Technical barriers like end-to-end encryption and disappearing messages further hinder efforts to detect harmful speech.[112]

Like hate speech, drug-related speech presents significant detection challenges, as identifying drug activity requires knowledge of context and inferences of intent that cannot be easily captured by automated content moderation methods.[113] People often speak about drugs in vague terms and use slang and coded language in drug transactions.[114] Simple keyword

---

> research or in jest, puts platforms in the difficult position of having to be subjective as to when they're required to report users.

Padilla Remarks, supra note 25, at 1:51–2:29.

110. See Sara Parker & Derek Ruths, Is Hate Speech Detection the Solution the World Wants?, 120 Proc. Nat'l Acad. Scis., no. 10, e2209384120, 2023, at 1, 1 (describing how "online hate speech has become the subject of substantial interest in the computer science community, inspiring groundbreaking research in machine learning (ML) that leverages deep learning and unsupervised methods to detect hate speech in ways and on scales unattainable by humans").

111. Id. Given these challenges, many platforms rely on users to report hate speech and do not rely solely, or even primarily, on automated detection. See id. at 3. But advances in machine learning techniques like self-supervision have enabled some platforms to proactively detect hate speech. See, e.g., Michael Auli, Matt Feiszli, Alex Kirillov, Holger Schwenk, Du Tran & Manohar Paluri, Advances in Content Understanding, Self-Supervision to Protect People, Meta (May 1, 2019), https://ai.meta.com/blog/advances-in-content-understanding-self-supervision-to-protect-people/ [https://perma.cc/4LMA-9E3E] ("[A]s we look to the long-term mission of keeping our platform safe, it will be increasingly important to create systems that can be trained using large amounts of unlabeled data.").

112. See Commission Report, supra note 2, at 22 (describing how platforms like B2B and social media sites, the darknet, and payment applications can facilitate fentanyl distribution); Leah Moyle, Andrew Childs, Ross Coomber & Monica J. Barratt, #Drugsforsale: An Exploration of the Use of Social Media and Encrypted Messaging Apps to Supply and Access Drugs, 63 Int'l J. Drug Pol'y 101, 102 (2019) ("[Wickr and WhatsApp] provide sellers with end-to-end encrypted communication to organise transaction details, and Wickr—alongside Kik, Telegram and Snapchat—has temporary photo and message capabilities that 'self-destruct' after a certain time period."); see also infra note 153 (citing NCMEC's concerns about the growing prevalence of encrypted communications and its impact on CSAM detection).

113. See Thomas Stackpole, Content Moderation Is Terrible by Design, Harv. Bus. Rev. (Nov. 9, 2022), https://hbr.org/2022/11/content-moderation-is-terrible-by-design (on file with the *Columbia Law Review*) ("Automation doesn't lend itself to moderation beyond rote cases such as spam or content that has already been identified in a database, because the work is nuanced and requires linguistic and cultural competencies.").

114. People usually do not search for drugs by name and often use "slang, street names of drugs, or other ways like misspelling, to evade being caught." Likes, Shares and Drug Deals: WVU Researchers Create Model that Detects Illicit Drug Trafficking on Social Media, WVU Today (Apr. 6, 2022), https://wvutoday.wvu.edu/stories/2022/04/06/likes-shares-and-drug-deals-wvu-researchers-create-model-that-detects-illicit-drug-trafficking-on-social-

filters—which many providers already use to block searches of drugs' exact names[115] and exclude hashtags promoting disordered eating[116]—do not effectively detect drug crimes since sellers and buyers rarely mention drugs by name (or spell them correctly).[117]

Nevertheless, the detection of online drug trafficking has become a popular area of machine learning research,[118] and some providers have successfully cracked down on drug sales using automated tools.[119] Researchers have examined the use of machine learning to detect drug dealing on Instagram,[120] Twitter,[121] and Google+.[122] Federal agencies have

---

media [https://perma.cc/K75S-3Z8N] (internal quotation marks omitted) (quoting Professor Xin Li) ; see also Hoffman, supra note 2 ("In a two-month span in the fall, the D.E.A. identified 76 cases that involved drug traffickers who advertised with emojis and code words on e-commerce platforms and social media apps."). Emojis and code words are also often used to signal illicit drugs on social media. See, e.g., Drug Enf't Admin., Emoji Drug Code: Decoded 1 (2021), https://www.dea.gov/sites/default/files/2021-12/Emoji%20Decoded.pdf [https://perma.cc/NC8T-F83B]; Drug Enf't Admin., Social Media: Drug Trafficking Threat 1–2 (2022), https://www.dea.gov/sites/default/files/2022-03/20220208-DEA_Social%20Media%20Drug%20Trafficking%20Threat%20Overview.pdf [https://perma.cc/SAQ3-9V3Y].

115. See, e.g., Instagram Blocks Some Drugs Advert Tags After BBC Probe, BBC (Nov. 7, 2013), https://www.bbc.com/news/technology-24842750 [https://perma.cc/2LCP-GVXM] (reporting that in 2013, Instagram blocked searches for certain terms associated with suspected illegal drug sales).

116. See, e.g., Talya Minsberg, Why Eating Disorder Content Keeps Spreading, N.Y. Times (Feb. 6, 2024), https://www.nytimes.com/2024/02/06/well/move/tiktok-legging-legs-eating-disorders.html (on file with the *Columbia Law Review*) (noting that TikTok banned the hashtag "#legginglegs" after the National Alliance for Eating Disorders flagged the trend to the company).

117. See, e.g., Rebecca Heilweil, AI Can Help Find Illegal Opioid Sellers Online. And Wildlife Traffickers. And Counterfeits., Vox (Jan. 21, 2020), https://www.vox.com/recode/2020/1/21/21060680/opioids-artificial-intelligence-illegal-online-pharmacies [https://perma.cc/99RQ-WQWK].

118. See, e.g., Tim K. Mackey, Janani Kalyanam, Takeo Katsuki & Gert Lanckriet, Twitter-Based Detection of Illegal Online Sale of Prescription Opioid, 107 Am. J. Pub. Health 1910, 1910 (2017) (using topic modeling, a type of statistical modeling that detects themes and patterns in a large set of texts, to identify words and phrases associated with fentanyl and other illegal opioid transactions).

119. Facebook's AI systems, for example, proactively detected more than four million pieces of drug sale content in Q3 2019. Mike Schroepfer, Community Standards Report, Meta (Nov. 13, 2019), https://ai.meta.com/blog/community-standards-report/ [https://perma.cc/4Y6Q-5UZS].

120. E.g., Jiawei Li, Qing Xu, Neal Shah & Tim K. Mackey, A Machine Learning Approach for the Detection and Characterization of Illicit Drug Dealers on Instagram: Model Evaluation Study, 21 J. Med. Internet Rsch., June 2019, at 1, 2.

121. E.g., Tim Mackey, Janani Kalyanam, Josh Klugman, Ella Kuzmenko & Rashmi Gupta, Solution to Detect, Classify, and Report Illicit Online Marketing and Sales of Controlled Substances via Twitter: Using Machine Learning and Web Forensics to Combat Digital Opioid Access, J. Med. Internet Rsch., Apr. 2018, at 1, 1.

122. E.g., Fengpan Zhao, Pavel Skums, Alex Zelikovsky, Eric L. Sevigny, Monica Haavisto Swahn, Sheryl M. Strasser & Yubao Wu, Detecting Illicit Drug Ads in Google+ Using Machine Learning, *in* Bioinformatics Research and Applications 171, 172 (Zhipeng Cai, Pavel Skums & Min Li eds., 2019).

also invested in AI to detect and disrupt online opioid sales.[123] While these technologies are imperfect[124]—and far less accurate than hash matching—automated technologies may one day be able to parse the coded language of drug transactions and accurately distinguish illegal from innocuous activity.[125]

B. *Complicating the CSAM Debate: The Cooper Davis Act's Novel Constitutional Issues*

Like the PROTECT Act, the Cooper Davis Act's efficacy and constitutionality will largely depend on whether and how the private search doctrine applies. This section explores these questions, which have arisen under the PROTECT Act but are complicated by non-CSAM detection under the proposed scheme.

1. *Does the Fourth Amendment Protect the Contents of Private Electronic Communications?* — Automated CSAM detection—which looks for illegal activity in users' private communications—has survived constitutional challenges, and courts have avoided addressing the question of whether an automated search of private communications constitutes a Fourth Amendment "search" because providers are not considered government agents under the PROTECT Act.[126] Consequently, without a finding of state action, courts need not determine whether the search implicates the

---

123. The FDA's budget allocates funding to create a "data warehouse" to facilitate data analytics, including machine learning algorithms, to assess trends in the opioid epidemic. Press Release, Scott Gottlieb, Comm'r, FDA, Statement From FDA Commissioner Scott Gottlieb, M.D. on the Agency's 2019 Policy and Regulatory Agenda for Continued Action to Forcefully Address the Tragic Epidemic of Opioid Abuse (Feb. 26, 2019), https://www.fda.gov/news-events/press-announcements/statement-fda-commissioner-scott-gottlieb-md-agencys-2019-policy-and-regulatory-agenda-continued (on file with the *Columbia Law Review*). The National Institute on Drug Abuse has also invested in creating an AI tool to detect illegal opioid sellers. FTC, Combatting Online Harms Through Innovation 20 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf [https://perma.cc/D2ZZ-HQHJ].

124. See Proactive Rate, supra note 106 ("[Meta's detection technology] is very promising but is still years away from being effective for all kinds of violations. For example, there are still limitations in the ability to understand context and nuance, especially for text-based content.").

125. See Li et al., supra note 120, at 10 (noting a "clear need for innovative technology solutions that have high accuracy and are scalable and can help . . . detect, classify, and take action against digital drug dealers"). In testimony before the House Energy and Commerce Committee in 2018, Meta Chief Executive Officer Mark Zuckerberg described the need to "build more AI tools that can proactively find [drug-related] content" given the sheer volume of content being shared on Facebook every day, which human content moderators alone cannot review. Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Com., 115th Cong. 58 (2018) (statement of Mark Zuckerberg, CEO, Meta).

126. See supra section I.B.2.

Fourth Amendment.[127] Many scholars have argued that even assuming hash searches for CSAM constitute state action, they would not be "searches" for Fourth Amendment purposes under two related rationales: the binary search doctrine and the third-party doctrine.

First, under the binary search doctrine, a minimally intrusive technique revealing only the presence or absence of contraband, such as a dog sniff, does not generate the same Fourth Amendment concerns as other kinds of searches since individuals do not have a reasonable expectation of privacy in possessing contraband.[128] Hash matching makes it possible for providers to identify the presence of CSAM with "near-perfect accuracy"[129] and does not expose the contents of files in the same way a visual review of an image or video does.[130] The only personal information hashing can disclose is a match to known CSAM—a match to contraband, in other words. As such, some consider hash matches analogous to dog sniffs,[131] which are not Fourth Amendment searches.[132]

Second, under the third-party doctrine, the Fourth Amendment does not protect what one has voluntarily turned over to a third party.[133] Under

---

127. See Orin S. Kerr, Terms of Service and Fourth Amendment Rights, 172 U. Pa. L. Rev. 287, 296 (2024) [hereinafter Kerr, Terms of Service] (noting that many cases challenging CSAM hashing have been resolved on state action grounds).

128. See United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding that "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest"); United States v. Place, 462 U.S. 696, 707 (1983) (explaining how a sniff by a narcotics detection dog "discloses only the presence or absence of narcotics, a contraband item" and that the information obtained by the search is "limited").

129. United States v. Miller, 982 F.3d 412, 418 (6th Cir. 2020). The odds of two different files coincidentally sharing the same hash value are "1 in 9,223,372,036,854,775,808." Id. at 430 (internal quotation marks omitted) (quoting United States v. Dunning, No. 15-cr-4-DCR-1, 2015 WL 1373616, at *2 (E.D. Ky. Oct. 1, 2015)).

130. See United States v. Keith, 980 F. Supp. 2d 33, 43 (D. Mass. 2013) ("[M]atching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file.").

131. See Laurent Sacharoff, The Binary Search Doctrine, 42 Hofstra L. Rev. 1139, 1182 (2014) ("Binary searches of computers present a pure form of a binary search, because they truly can disclose the presence or absence of contraband only without revealing other information, and often, with almost no physical intrusion whatsoever."); Kevin Groissant, Note, Should Warrantless Digital Searches Be Allowed to Decrease the Dissemination of Child Pornography: A Likely Future for Private and Governmental Use of Hash Value Algorithms, 56 Creighton L. Rev. 569, 590 (2023) (noting that the Supreme Court has not ruled on whether a hash value algorithm constitutes a Fourth Amendment search); Anirudh Krishna, Note, Internet.gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse, 109 Calif. L. Rev. 1581, 1628–30 (2021) (arguing that PhotoDNA scans are "quite similar to drug-sniffing dogs"); see also Dennis Martin, Note, Demystifying Hash Searches, 70 Stan. L. Rev. 691, 717–21 (2018) (arguing that hash searches violate the Fourth Amendment if they are used to look for evidence outside the scope of a search warrant or other permissive mechanism).

132. *Place*, 462 U.S. at 707.

133. See *Jacobsen*, 466 U.S. at 117 ("It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that

this theory, searches of a user's private electronic communications transmitted via providers—such as cloud storage uploads, emails, and messages—are not Fourth Amendment searches because a user has reduced privacy interests in information they knowingly share with providers.[134] The third-party doctrine shares the same basic rationale as the private search exception: Both rely on the principle that "[a] private search extinguishes an individual's reasonable expectation of privacy in the object searched."[135]

But these arguments do not easily map onto automated searches for drug and other non-CSAM crimes.[136] First, (hard) hashing for CSAM is a rare example of a digital binary search. Possession of online CSAM is a crime regardless of context,[137] whereas most other online crimes require some degree of context to discern.[138] No other type of automated search can reveal solely the presence or absence of contraband, and nothing more.[139] Second, whether the third-party doctrine applies to the contents

---

information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the Fourth Amendment does not protect information disclosed to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

134. See Smith v. Maryland, 442 U.S. 735, 744 (1979) ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information . . . . In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."); Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 581–89 (2009) [hereinafter Kerr, Third-Party Doctrine].

135. Priscilla Grantham Adams, Nat'l Ctr. for Just. & Rule of L., Fourth Amendment Applicability: Private Searches 1–2 (2008), https://www.neshaminy.org/cms/lib6/PA01000466/Centricity/Domain/223/Private%20Search%20Doctrine.pdf [https://perma.cc/D23L-N4AJ]; see also *Jacobsen*, 466 U.S. at 117 (noting that the private search doctrine "follows from the analysis applicable when private parties reveal other kinds of private information to the authorities").

136. While courts need not resolve the issue of whether hashing constitutes a search in CSAM cases, it is harder to avoid under the Cooper Davis Act since providers may be considered government agents whose searches are subject to the Fourth Amendment. See infra section II.B.2.

137. 18 U.S.C. § 2252A(a)(2) (2018) (criminalizing the knowing receipt or distribution of child pornography); id. § 2252A(a)(5) (criminalizing the knowing possession of or access with intent to view child pornography).

138. See supra section II.A. Possession of a picture of drugs, for example, is not itself a crime.

139. The binary search doctrine has also attracted criticism for being inconsistent with the Court's Fourth Amendment jurisprudence. See, e.g., Lawrence Rosenthal, Binary Searches and the Central Meaning of the Constitution, 22 Wm. & Mary Bill Rts. J. 881, 920–21 (2014) (arguing that the doctrine "places to one side the most powerful pragmatic argument that is ordinarily advanced in favor of Fourth Amendment restraint on investigatory power—the claim that we must inhibit the ability of the government to gather evidence against the guilty in order to protect the innocent").

of private communications transmitted via third-party providers is an open question, as the Supreme Court has not directly addressed the issue.[140]

The Second and Sixth Circuits are the only Courts of Appeals to address the question.[141] In *United States v. Warshak*, the Sixth Circuit held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial [internet service provider].'"[142] The court emphasized that it would "defy common sense" for the Fourth Amendment to afford less protection to email compared to traditional forms of communication; the court then held that the third-party doctrine did not apply to an internet service provider, which, like a post office or telephone company, was not the intended recipient of the private communications.[143] In 2024, the Second Circuit formally adopted *Warshak*—confirming what it had previously assumed—holding "that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry."[144] Federal district courts across the country have also applied *Warshak*'s logic to providers like Facebook.[145]

The Department of Justice has also adopted a policy of obtaining a warrant whenever it seeks the content of user emails or other "similar stored content" from a provider—seemingly in accordance with *Warshak* (or in acquiescence to its influence).[146] And on the provider side, many

---

140. See, e.g., Rehberg v. Paulk, 611 F.3d 828, 847 (11th Cir. 2010) ("No Supreme Court decision . . . defines privacy rights in email content voluntarily transmitted over the global Internet and stored at a third-party [internet service provider]."), aff'd on other grounds, 566 U.S. 356 (2012). The closest the Supreme Court has come to addressing the question was in *City of Ontario v. Quon*, in which the Court assumed arguendo that a police officer had a reasonable expectation of privacy in text messages he sent on his work pager. 560 U.S. 746, 750 (2010). Declining to resolve the question, the Court cautioned against "elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." Id. at 759.

141. See United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (noting that the Fourth Amendment protects the content of emails); see also United States v. Maher, 120 F.4th 297, 307–08 (2d Cir. 2024) (following *Warshak*); cf. Schuchardt v. President of the U.S., 839 F.3d 336, 346 (3d Cir. 2016) (holding that plaintiff had "a constitutional right to maintain the privacy of his personal [electronic] communications, online or otherwise" for purposes of establishing injury-in-fact for Article III standing).

142. *Warshak*, 631 F.3d at 288 (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)).

143. Id. at 285–86.

144. *Maher*, 120 F.4th at 307 (internal quotation marks omitted) (quoting United States v. Hasbajrami, 945 F.3d 641, 666 (2d Cir. 2019)).

145. See, e.g., United States v. Chavez, 423 F. Supp. 3d 194, 203 (W.D.N.C. 2019) (citing *Warshak* in holding that defendant had a reasonable expectation of privacy in nonpublic content on his Facebook account); see also United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (agreeing with *Warshak*'s conclusion that "individuals have a reasonable expectation of privacy in the content of emails").

146. See Elana Tyrangiel, Acting Assistant Att'y Gen., Testimony Before the House Judiciary Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations, DOJ (Mar. 19,

companies require a warrant before disclosing user content to law enforcement.[147] Still, the Supreme Court has not formally blessed *Warshak* nor decided whether a reasonable expectation of privacy exists in the contents of private electronic communications.[148]

2. *Does the Cooper Davis Act Convert Providers Into Government Agents?* — Under lower courts' varying government agency tests, providers are universally considered private parties under the PROTECT Act.[149] But their status under the Cooper Davis Act is less clear, as two features of the proposed bill complicate the state action question: (1) the prohibition of deliberate blindness to violations and (2) the direct reporting channel to the DEA.

First, the Cooper Davis Act goes further than its model statute, prohibiting providers from deliberately turning a blind eye to "readily apparent" violations.[150] The Cooper Davis Act also imposes more severe penalties for violations: Failure to comply with the law is considered a criminal offense.[151] The bill imposes fines of up to $190,000 for initial violations and up to $380,000 for subsequent violations and, unlike its model statute, fines of up to $100,000 for submitting false or fraudulent information in reports to the DEA or omitting information that was reasonably available.[152] What constitutes blindness under the law is also

---

2013), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-elana-tyrangiel-testifies-us-house-judiciary [https://perma.cc/6QGC-PMYK] (recognizing the "appeal" of requiring law enforcement to obtain a warrant to compel disclosure of emails and similar stored content information from a provider). The FBI's Domestic Investigations and Operations Guide provides that "[c]ontents in 'electronic storage' (e.g., unopened e-mail/voice mail) require a search warrant." FBI, Domestic Investigations and Operations Guide § 18.7.1.3.4.4 (2021), https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2021-version/fbi-domestic-investigations-and-operations-guide-diog-2021-version-part-2-of-3/ (on file with the *Columbia Law Review*).

147. See Ctr. for Democracy & Tech., Analysis of Department of Justice March 19, 2013 ECPA Testimony 2 n.4 (2013), https://cdt.org/wp-content/uploads/pdfs/Analysis%20of%20DOJ%20ECPA%20testimony.pdf [https://perma.cc/935K-VSCC] ("Leading Internet companies, including Google, Facebook, Microsoft, Twitter and Yahoo!, have all announced that they follow the *Warshak* rule nationwide . . . ."); Ira S. Rubinstein, Gregory T. Nojeim & Ronald D. Lee, Systematic Government Access to Personal Data: A Comparative Analysis, 4 Int'l Data Priv. L. 96, 115 (2014) (noting that "service providers and the Justice Department now seem to agree that a judicial warrant is needed to compel third-party disclosure of content.").

148. See supra note 140 and accompanying text.

149. See supra section I.B.2.

150. Cooper Davis Act, S. 1080, 118th Cong. § 2 (2023) (adding § 521(g)(4) to Part E of the Controlled Substances Act); see also supra note 44 (comparing the language of the statutes).

151. S. 1080 § 2 (adding § 521(f)(1)(A)). Under the PROTECT Act, providers are subject only to fines. See 18 U.S.C. § 2258A(e) (2018).

152. S. 1080 § 2 (adding § 521(f)(1)(B), (f)(2)). Providers that fail to make required reports under the PROTECT Act are subject to fines of up to $150,000 for initial violations and $300,000 for subsequent violations. 18 U.S.C. § 2258A(e).

unclear, which may lead risk-averse providers to report suspected violations more aggressively than they otherwise would to avoid incurring penalties.[153] The bill therefore places more pressure on providers to report than the PROTECT Act, creating a more coercive regulatory scheme.

Second, the Cooper Davis Act requires providers to report to a federal law enforcement agency, rather than to an intermediary private nonprofit like NCMEC, creating a direct connection between the government and private companies—similar to the reporting law at issue in *Skinner*.[154] Together, the bill's antiblindness provision and direct reporting channel to the DEA impose an affirmative obligation on providers that extends beyond what is required of them under the PROTECT Act. While the Cooper Davis Act places no obligation on providers to search for drug activity on their sites, the law may nevertheless have the "*de facto* effect of leading to proactive monitoring"[155]—much like how recent content regulations in the European Union have pushed providers to adopt more automated detection tools.[156] Compliance with the proposed bill would likely lead to overdeletion and overreporting of lawful content. Particularly in an area of rapidly developing technology like machine learning, legislation like the Cooper Davis Act that indirectly encourages automation may have the unwanted effect of pushing providers to adopt more complex technologies sooner than they otherwise would.[157]

---

153. In response to concerns that the government would consider end-to-end encryption a form of deliberate blindness, the 2024 House bill added a provision noting that nothing in the bill shall be construed to "prohibit a provider from using end-to-end encryption or require a provider to decrypt encrypted communications." H.R. 8918, 118th Cong. § 2 (2024) (adding § 521(g)(5) to Part E of the Controlled Substances Act).

Many privacy advocates and criminal justice groups had criticized the Senate bill's blindness provision as encouraging platforms to undermine encryption features "out of the fear that law enforcement will argue that, by taking themselves out of the loop and allowing all users to have truly secure conversation[s], providers are 'blinding' themselves" from violations. India McKinney & Andrew Crocker, Amended Cooper Davis Act Is a Direct Threat to Encryption, Elec. Frontier Found. (July 20, 2023), https://www.eff.org/deeplinks/2023/07/amended-cooper-davis-act-direct-threat-encryption [https://perma.cc/K4LN-28QM]. NCMEC has also warned that, based on its communications with providers, it "anticipates that widespread adoption of end-to-end encryption by reporting [providers] will begin at some point in CY 2024 and could result in a loss of up to 80% of NCMEC's CyberTipline reports." OJJDP Report, supra note 31, at 3.

154. See supra notes 50–56 and accompanying text.

155. See Bloch-Wehba, Automation in Moderation, supra note 13, at 67.

156. See id. at 65–67 (describing how European regulations like Article 17 of the EU Copyright Directive and Germany's Network Enforcement Act of 2018 have pushed platforms toward adopting automated screening tools to identify illegal content, even though these laws explicitly disclaim any requirement of proactive monitoring or screening); see also The Text of Article 13 and the EU Copyright Directive Has Just Been Finalised, Felix Reda (Feb. 13, 2019), https://felixreda.eu/2019/02/eu-copyright-final-text/ [https://perma.cc/X87C-D9RF] (stating that under these provisions, service providers "will have no choice but to deploy upload filters" to block infringing content).

157. See Bloch-Wehba, Automation in Moderation, supra note 13, at 75 ("As it stands, automated content moderation already demonstrates the risk that technical 'solutions'

Regardless of whether the Cooper Davis Act is enacted, questions of government agency may well come before the courts, as Congress has demonstrated an interest in expanding providers' obligations regarding online CSAM.[158] In a world in which "police outsource surveillance to private third parties"[159]—third parties with access to scores of potentially incriminating and deeply personal information—the question of when

---

designed to prevent bad content from spreading will have collateral effects on lawful expression.").

158. In 2023, senators introduced two bills aimed at cracking down on the proliferation of CSAM online by imposing greater obligations on providers. The first, the EARN IT Act, is a highly controversial bill that would strip providers of Section 230 immunity for civil claims for injuries involving CSAM and require providers to adhere to "best practices" aimed at combating CSAM. See EARN IT Act of 2023, S. 1207, 118th Cong. (2023). The EARN IT Act was first introduced in 2020 and reintroduced in 2022. See S. 3538, 117th Cong. (2022); S. 3398, 116th Cong. (2020). Many argue that the EARN IT Act presents a serious threat to user privacy and would deputize providers as government agents. See, e.g., Sophia Cope, Aaron Mackey & Andrew Crocker, The EARN IT Act Violates the Constitution, Elec. Frontier Found. (Mar. 31, 2020), https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution [https://perma.cc/W45U-NTN4]; see also Krishna, supra note 131, at 1618 (arguing that the Act would convert technology companies into government agents).

The second bill, the STOP CSAM Act of 2023, would increase liability for providers who promote, facilitate, host, store, or make available CSAM on their platforms; like the EARN IT Act, the STOP CSAM Act would remove providers' Section 230 immunity. See S. 1199, 118th Cong. (2023). The Senate Judiciary Committee approved the EARN IT and STOP CSAM Acts in May 2023, referring both to the full Senate. Press Release, Lindsey Graham, U.S. Sen. for S.C., Senate Judiciary Committee Unanimously Approves EARN IT Act (May 4, 2023), https://www.lgraham.senate.gov/public/index.cfm/press-releases?ID=5A0FDDE3-8F28-4A41-803A-92F38D2F2BA2 [https://perma.cc/K7W4-93XD]; Press Release, S. Comm. on the Judiciary, Senate Judiciary Committee Advances Durbin's STOP CSAM Act to Crack Down on the Proliferation of Child Sex Abuse Material Online (May 11, 2023), https://www.judiciary.senate.gov/press/dem/releases/senate-judiciary-committee-advances-durbins-stop-csam-act-to-crack-down-on-the-proliferation-of-child-sex-abuse-material-online [https://perma.cc/B8D7-3ULH].

Some privacy advocates and senators have criticized both bills for many of the same reasons they oppose the Cooper Davis Act—threats to encrypted communications, user privacy, and free speech. See Letter from Civil and LGBTQ+ Rights Groups to Chuck Schumer, S. Majority Leader (Sept. 25, 2023), https://www.aclu.org/wp-content/uploads/2023/09/STOP-CSAM-Sign-On-Letter6.pdf [https://perma.cc/DSY5-ZT43]; EFF Letter From Elec. Frontier Found. to Richard Durbin, Chairman, S. Comm. on the Judiciary & Lindsey Graham, Ranking Member, S. Comm. on the Judiciary (May 1, 2023), https://www.eff.org/document/eff-letter-senate-judiciary-committee-vote-no-earn-it-act-and-stop-csam-act [https://perma.cc/Y2Y3-2CVH]; Chamber of Progress, Senate Democrats Raise Issues With EARN IT, Stop CSAM and Cooper Davis Acts, YouTube (May 11, 2023), https://www.youtube.com/watch?v=52Nk9PttmdE (on file with the *Columbia Law Review*). The ACLU, for example, has urged the Senate Judiciary Committee to reject all three bills. Letter from Christopher Anders, Fed. Pol'y Dir., ACLU, Jenna Leventoff, Senior Pol'y Couns., ACLU & Cody Venzke, Senior Pol'y Couns., ACLU, to Dick Durbin, S. Comm. on the Judiciary & Lindsey Graham, Ranking Member, S. Comm. on the Judiciary (May 3, 2023), https://www.aclu.org/wp-content/uploads/2023/05/ACLU-Letter-EARN-It-STOP-CSAM-Cooper-Davis-May-17-202363.pdf [https://perma.cc/GL9G-HR39].

159. Paul Ohm, The Fourth Amendment in a World Without Privacy, 81 Miss. L.J. 1309, 1338 (2012).

third parties become state actors "may now be the most consequential quandary in Fourth Amendment jurisprudence."[160]

3. *What Is the Scope of an Automated Private Search?* — Assuming the Cooper Davis Act does not convert providers into state actors subject to the Fourth Amendment, the law's efficacy will depend on the scope of the private search exception—an issue that has created a circuit split in certain CSAM cases.[161] Imagine Provider A develops a highly accurate machine learning algorithm to detect fentanyl transactions in users' direct messages. When the algorithm gets a hit, a content moderator employed by Provider A confirms that it meets the requisite standard for reporting before sending the messages, as well as the user's information, to the DEA. Imagine Provider B uses the same algorithm, but when it gets a hit, it automatically reports the user's messages and information to the DEA.

For Provider A, it is clear under either the sui generis or first-look approach that the DEA may view the messages without a warrant since it would learn no more than what the moderator already knew from their search; this is akin to a detective viewing images that a provider identified through hash matching and visually confirmed to be CSAM before reporting.[162] But for Provider B, the answer is less clear under the sui generis approach. Under the Cooper Davis Act, there is no private intermediary between providers and the DEA that can extinguish a user's privacy interest in their information before it reaches the government, making it harder for courts to avoid the question of what it means for the government to exceed the provider's private search—the same question that has created a circuit split in online CSAM cases.[163]

Regardless of whether the Cooper Davis Act is enacted, the question of the private search doctrine's applicability to automated searches is already a live issue. Many providers currently use complex fuzzy hashing algorithms to detect previously unseen CSAM.[164] While courts (on both sides of the circuit split) have relied on the "near-perfect accuracy" of hash

---

160. Christopher Slobogin, "Volunteer" Searches, 85 U. Pitt. L. Rev. 1, 4 (2023) (arguing that the government can work around the Fourth Amendment's restrictions "simply by asking or paying" private companies for users' personal information without triggering state action); see also Joseph Zabel, Public Surveillance Through Private Eyes: The Case of the EARN IT Act and the Fourth Amendment, 2020 U. Ill. L. Rev. Online 167, 168, https://www.illinoislawreview.org/wp-content/uploads/2020/08/Zabel.pdf [https://perma.cc/5WJN-PDPZ] ("[T]he inquiry as to whether or not a private actor has been deputized has become far less straightforward as law enforcement consumes more and more data from private enterprises.").

161. See supra section I.C.

162. See supra note 66.

163. See supra section I.C.

164. See, e.g., Google Tools, supra note 35 ("For many years, Google has been working on machine learning classifiers to allow us to proactively identify never-before-seen CSAM imagery so it can be reviewed and, if confirmed as CSAM, removed and reported as quickly as possible.").

matching for CSAM,[165] these arguments apply best to hard hashing, which requires an exact match to known CSAM hashes.[166] On the other hand, fuzzy hashing to identify never-before-seen CSAM carries the inherent risk of incorrectly matching two files.[167] Courts have glossed over the distinction between hard and fuzzy hashing algorithms, touting the accuracy of "hashing" without specifying which kind.[168] To be sure, many fuzzy hashing algorithms, including Microsoft's PhotoDNA technology, are highly reliable and accurate,[169] and they offer significant practical benefits since they can identify new and AI-generated CSAM,[170] rather than being limited to known CSAM that has been reported, viewed, classified, hashed, and entered into a database. But it is not obvious that the sui generis approach applies with the same force to fuzzy hashing algorithms, which lack many of the characteristics that courts have relied on when justifying the sui generis approach[171]—most importantly, fuzzy hashing algorithms identify "matches" even when the exact contents of a file have never been viewed before. Under the sui generis approach, may the government constitutionally view files identified solely by a fuzzy hashing algorithm, which no private party has confirmed to be CSAM?

III. A PRIVATE SEARCH DOCTRINE FOR MODERN CRIME-DETECTION ALGORITHMS

The Cooper Davis Act highlights issues that have largely been avoided in the government's fight against online CSAM because of the PROTECT Act's reporting scheme and the exceptional qualities of hash matching for CSAM.[172] This Part assesses the Fourth Amendment issues raised by the proposed bill and discusses the implications of treating providers as government agents. If the Fourth Amendment protects the contents of private electronic communications and the Cooper Davis Act converts providers into state actors—issues discussed in sections III.A and III.B, respectively—then providers would need to obtain search warrants before searching for drug-related activity. This would effectively defang the

165. United States v. Miller, 982 F.3d 412, 418 (6th Cir. 2020); see also supra section I.C.1 (describing the sui generis approach).

166. See supra text accompanying note 36.

167. See supra text accompanying note 39.

168. No federal court has addressed perceptual or fuzzy hashing in the CSAM context. Cf. Intel Corp. v. Rivers, No. 2:18-cv-03061-MCE-AC, 2019 WL 4318583, at *2 (E.D. Cal. Sept. 12, 2019) (mentioning fuzzy hash searches of emails for alleged sharing of trade secrets).

169. See supra notes 34–35.

170. See Drew Harwell, AI-Generated Child Sex Images Spawn New Nightmare for the Web, Wash. Post (June 19, 2023), https://www.washingtonpost.com/technology/2023/06/19/artificial-intelligence-child-sex-abuse-images/ (on file with the *Columbia Law Review*) (reporting the rise in AI-generated CSAM).

171. See, e.g., supra note 129 and accompanying text (emphasizing the near certainty that hashed files contain CSAM).

172. See supra section I.B.

Cooper Davis Act since providers would often have no basis for probable cause to perform ex ante surveillance of users.

On the other hand, if the Cooper Davis Act maintains providers' status as private actors, then the government would be able to use all the information that providers are required to report to the DEA, so long as it does not exceed the scope of the private search—a situation that, by design, would bring an immense volume of previously inaccessible information about users into the government's hands.[173] Section III.C argues that if such cases arise, courts should adopt the "first-look" view of the private search exception because it is the approach most consistent with the principles underlying the Supreme Court's private search doctrine.

A. *Fourth Amendment Protection of the Contents of Private Electronic Communications*

While many have argued that users lack a reasonable expectation of privacy in information revealed by a hash match for CSAM under the binary search and third-party doctrines,[174] these doctrines should not prevent courts from recognizing that the contents of private communications sent using third-party providers fall within the Fourth Amendment's ambit.

1. *Inapplicability of the Binary Search Doctrine to Searches for Drug Crimes*. — First, the binary search doctrine is inapposite to searches for drug crimes, which necessarily involve user speech.[175] Most importantly, searches for drug crimes do not provide information in binary in the same way dog sniffs and CSAM hashing do. The target drug offenses require context to discern, and automated searches for drug-related activity reveal far more than the mere presence or absence of contraband. Much like hate speech, the presence of online drug-related "contraband" is bound up with the presence of protected speech.[176] Searches for drug crimes may therefore reveal *unlimited* amounts of innocuous information in which users have a legitimate expectation of privacy, whereas dog sniffs do not constitute searches precisely because they are "limited both in the manner

---

173. See supra notes 6–7 and accompanying text.

174. See supra section II.B.1.

175. See supra notes 114–117 and accompanying text.

176. See supra notes 109–111 and accompanying text; see also 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, 1313 (2019) (arguing that hash matching is "qualitatively different from other types of binary authentication"). Many consider hashing to be more accurate at detecting the presence of contraband than dog sniffs and spot tests. See, e.g., Robyn Burrows, Comment, Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files, 19 Geo. Mason L. Rev. 255, 279 (2011) ("Hashing is actually much more accurate than a dog sniff since it is almost mathematically impossible to mistake one file for another.").

in which the information is obtained and in the content of the information revealed."[177] Thus, automated searches for drug crimes—as contemplated by the Cooper Davis Act—cannot be treated as the digital equivalent of a dog sniff.[178] And even assuming arguendo CSAM hashing falls under the binary search doctrine, proactive detection of drug-related speech constitutes a far more intrusive search, potentially exposing the contents of user communications rather than a mere match to known illicit material.

2. *Problems With Extending the Third-Party Doctrine.* — As an initial matter, it would be strange to apply the third-party doctrine to providers when this inquiry assumes that those same providers are acting as government agents (since the Fourth Amendment applies only to state action).[179] Ignoring that wrinkle, the Supreme Court has never applied the third-party doctrine to the contents of private electronic communications,[180] and in recent years, the Court has expressed reluctance to liberally apply the third-party doctrine to personal information shared with modern electronic communications services, given the ubiquity of third-party providers in everyday life. In *Carpenter v. United States*, the Court declined to apply the third-party doctrine to cell-site location information (CSLI), even though the government had obtained that information from third parties, and it recognized "a legitimate expectation of privacy in the record of [one's] physical movements as captured through CSLI."[181]

Carpenter marked an important shift in the Court's application of the "reasonable expectation of privacy" test, as the Court paid close attention to what *kind* of information a search might reveal, moving away from its traditional focus on the *source* of the information or the *actions* law enforcement took to obtain the information.[182] The Court emphasized

177. United States v. Place, 462 U.S. 696, 707 (1983).

178. The title of this Note, *Digital Dog Sniffers*, invokes this question of whether automated detection of drug crimes could be considered a kind of "digital dog sniff." The title also reflects how the Cooper Davis Act incentivizes providers to proactively search for drug crimes, much like sniffer dogs in a figurative sense. Some student scholarship has used the term "digital dog sniff" in the context of CSAM hashing. See Burrows, supra note 176, at 258; Martin, supra note 131, at 693.

179. See Krishna, supra note 131, at 1632 (considering whether tech companies might be "double agent[s]—providing both a messaging service to users and a law enforcement service to the government").

180. See supra notes 140–148 and accompanying text.

181. 138 S. Ct. 2206, 2217 (2018).

182. See Orin S. Kerr, The Digital Fourth Amendment 154–55 (2024) ("Before *Carpenter*, whether a Fourth Amendment search was recognized depended on the place or thing serving as the information source. *Carpenter* embarks on a different path. It imbues constitutional protection upon information outside of any places or things."); Paul Ohm, The Many Revolutions of *Carpenter*, 32 Harv. J.L. & Tech. 357, 385–86 (2019) (arguing that *Carpenter*'s multi-factor test will produce more predictable outcomes than the "reasonable expectation of privacy" test and empower courts "to propound a normative vision for the kind of society the [Fourth Amendment] seeks to protect").

that CSLI provides a detailed record of an individual's physical movements every day, every moment, and potentially over several years—implicating privacy concerns "far beyond those considered" in prior cases.[183] (*Carpenter*'s holding, however, was limited to the particular facts of the case, which involved the acquisition of more than six days of CSLI data; the Court declined to "decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny."[184])

Still, some have argued that the third-party doctrine should apply to providers since individuals consent to providers scanning their messages and disclosing illegal content in limited circumstances; users typically agree to terms of service that waive their right to privacy in their communications when it comes to detecting spam and CSAM.[185] But the notions of voluntariness and consent in which the third-party doctrine finds its basis are more questionable in the digital age, "in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[186] Terms of service should not

---

183. *Carpenter*, 138 S. Ct. at 2220 (referencing Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976)).

184. Id. at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

185. See, e.g., Kerr, Third-Party Doctrine, supra note 134, at 588 (arguing that "[t]hird-party disclosure eliminates privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy"). Some district courts have cited terms of service to justify concluding that users lack a reasonable expectation of privacy in their communications via third-party providers. Compare United States v. Montijo, No. 2:21-cr-75-SPC-NPM, 2022 WL 93535, at *7 (M.D. Fla. Jan. 10, 2022) (holding that the defendant did not have a reasonable expectation of privacy in his Facebook Messenger communications based in part on the fact that Facebook, in its terms of service, gave "fair warning" that users risked being reported to law enforcement or NCMEC if the platform discovered CSAM), with *In re Search of: Encrypted Data*, No. 20-sw-321 (ZMF), 2021 WL 2100997, at *4 (D.D.C. May 22, 2021) (noting that individuals "generally have reasonable expectations of privacy in the emails that they send through commercial providers like Google" despite providers having terms of service that prohibit using their platforms to violate the law (internal quotation marks omitted) (quoting United States v. Miller, 982 F.3d 412, 426 (6th Cir. 2020))).

186. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); see also *Carpenter*, 138 S. Ct. at 2220 (noting that since virtually any activity on a phone can generate CSLI, this information is not truly "shared" with a third party); id. at 2263 (Gorsuch, J., dissenting) ("Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government*."); Orin S. Kerr, Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805, 813 (2003) (arguing that the internet presents unique Fourth Amendment challenges because it "does not protect information that has been disclosed to third-parties, and the Internet works by disclosing information to third-parties").

Most people also accept terms of service without ever reading them. See Jonathan A. Obar & Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, 23 Info., Commc'n & Soc'y 128,

dictate the Fourth Amendment's applicability since such agreements define legal relationships among private parties, not between individuals and the government.[187] In line with *Carpenter*'s protection of sensitive personal information "shared" with third parties, courts should instead recognize a reasonable expectation of privacy in the communications that individuals send via providers, regardless of terms of service.[188] The third-party doctrine should apply only when individuals voluntarily disclose information online to the public, *not* to private recipients—for example, when users publish posts on social media that are visible to the public, they voluntarily disclose that information and assume the risk that the government may obtain and use it.[189]

B. *Reconsidering Government Agency*

Assuming the Fourth Amendment protects the information targeted by providers' searches for drug crimes, providers would still be subject to the Fourth Amendment only if they are agents or instruments of the government.[190] One member of the Senate Judiciary Committee has warned that the Cooper Davis Act "effectively deputize[s]" providers to serve as law enforcement.[191]

As the Supreme Court has repeatedly stated, whether a private party becomes a state actor is a "necessarily fact-bound inquiry,"[192] so it is

---

143 (2020) (finding that more than ninety-eight percent of survey participants missed a clause about their data being shared with the NSA).

187. See United States v. Maher, 120 F.4th 297, 308 (2d Cir. 2024) (holding that "Google's particular Terms of Service—which advise that Google 'may' review users' content—did not extinguish [defendant's] reasonable expectation of privacy in that content as against the government" (citation omitted)); Kerr, Terms of Service, supra note 127, at 288–97 (calling the argument that terms of service define Fourth Amendment rights a "syllogism"). In *Maher*, the Second Circuit also noted that in a different context, the Supreme Court had "declined to construe even unqualified language in a private contract as extinguishing a person's expectation of privacy as against the government." *Maher*, 120 F.4th at 309 (citing Byrd v. United States, 584 U.S. 395 (2018)).

188. *Carpenter* is consistent with *Warshak* and suggests the Court's willingness to confer Fourth Amendment protection onto private electronic communications, which, like CSLI, contain detailed and extensive personal information. See Jesse Lieberfeld & Neil Richards, Fourth Amendment Notice in the Cloud, 103 B.U. L. Rev. 1201, 1207 (2023) ("In the 2018 case of *Carpenter v. United States*, the Court tacitly affirmed *Warshak*'s central holding . . . ." (footnotes omitted)); see also *Carpenter*, 138 S. Ct. at 2269 (Gorsuch, J., dissenting) (describing third-party doctrine cases like *Smith* and *Miller* as cases that under a *Katz* analysis "extinguish Fourth Amendment interests once records are given to a third party," whereas "property law may preserve them").

189. Courts should also respect the line between content and noncontent, dating back to the nineteenth century. See supra note 48 and accompanying text. Individuals' speech, even speech related to drug transactions, falls squarely within the "content" category.

190. See supra note 54 and accompanying text.

191. Padilla Remarks, supra note 25, at 2:33.

192. Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 298 (2001) (internal quotation marks omitted) (quoting Lugar v. Edmonson Oil Co., 457 U.S. 922, 939 (1982)).

impossible to declare with certainty how courts would treat providers under the Cooper Davis Act since the courts of appeals use different tests for determining government agency, which would all turn on the how the bill is ultimately interpreted and enforced. This section explores how lower courts might consider state action under the predominant "critical factors" test. After concluding that courts would likely maintain providers' status as private parties under the bill, this section then offers guiding principles for evaluating the law's enforcement, taking notice of the significant threat of surrogate surveillance by providers that this bill poses.

1. *Applying the Lower Courts' Government Agency Tests.* — Under existing formulations of Fourth Amendment state action, lower federal courts are unlikely to consider providers to be state actors under the proposed bill, just as they decline to do so vis-à-vis the PROTECT Act.[193] Although the bill undoubtedly reflects the government's awareness and indirect encouragement of providers searching for drug-related activity, "[m]ere governmental authorization of a particular type of private search in the absence of more active participation or encouragement" does not satisfy the first prong of the critical factors test—government knowledge and acquiescence.[194] The proposed bill does not require providers to affirmatively search for drug-related crimes, and even a prohibition of deliberate blindness to violations does not amount to explicit direction, which courts have required for this prong to be met.[195]

As for the second factor, assuming the bill is enacted, it is difficult to argue that providers would search for drug-related content with the intent of assisting law enforcement since many platforms already proactively detect this content in the absence of any reporting requirements.[196] Private parties may have a dual motive to assist law enforcement without implicating the Fourth Amendment as long as they have "a legitimate, independent motivation."[197] Similar to their interest in eradicating CSAM,[198] providers have a legitimate, independent interest in rooting out illegal drug activity on their sites, particularly given mounting public scrutiny of their role in the opioid crisis (which itself motivated lawmakers to propose the legislation at issue).[199] This interest likely negates the

193. See supra section I.B.2.

194. See United States v. Rosenow, 50 F.4th 715, 731 (9th Cir. 2022) (alteration in original) (internal quotation marks omitted) (quoting United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981)).

195. See, e.g., United States v. Sykes, 65 F.4th 867, 877 (6th Cir. 2023) (holding that the government did not compel Facebook's actions); *Rosenow*, 50 F.4th at 742 (holding that the government did not incentivize, direct, or encourage Yahoo's investigatory efforts); see also supra note 59 and accompanying text.

196. See supra note 119 and accompanying text.

197. *Rosenow*, 50 F.4th at 733 (citing United States v. Cleaveland, 38 F.3d 1092, 1094 (9th Cir. 1994)).

198. See supra note 60 and accompanying text.

199. See, e.g., Louise Matsakis & Kate Snow, Snapchat Makes It Harder for Kids to Buy Drugs, NBC News (Jan. 18, 2022), https://www.nbcnews.com/tech/social-media/snapchat-

second critical factor.[200] Furthermore, court determinations of intent often rely on how a provider justifies its actions in declarations or suppression hearing testimony, and courts have given broad deference to corporate leaders in establishing intent.[201]

Even adopting the Tenth Circuit's flexible application of the "critical factors" test in *United States v. Ackerman*—arguably the broadest circuit court conception of Fourth Amendment state action—courts would likely reach the same conclusion.[202] At a high level of generality, providers might act with the government's consent and to further the government's goals, but providers could argue any number of alternative intents besides aiding law enforcement.[203] For one, providers could assert that hosting drug advertising and distribution on their sites is bad for business. So, even under their differing applications of the "critical factors," courts would likely consider providers to be private actors since the Cooper Davis Act does not explicitly require them to search for drug crimes and providers may have multiple motivations driving their automated detection—irrespective of the bill's coercive features.

2. *Guiding Agency Principles.* — Courts must apply workable and predictable government agency standards that give providers notice of their potential Fourth Amendment obligations and give users clarity regarding the scope of their Fourth Amendment rights when using these ubiquitous communication services.

---

makes-harder-kids-buy-drugs-rcna12652 (on file with the *Columbia Law Review*) (describing internal changes Snapchat made following public scrutiny over the number of teenagers buying drugs on the platform); see also Marshall Press Release, supra note 7 (describing how the growing trend of teenagers buying drugs on social media inspired the introduction of the Cooper Davis Act); Shaheen Press Release, supra note 6 (same).

200. As the Seventh Circuit has noted, "this sort of activity is analogous to shopkeepers that have sought to rid their physical spaces of criminal activity to protect their businesses." United States v. Bebris, 4 F.4th 551, 562 (7th Cir. 2021) (citing United States v. Miller, 982 F.3d 412, 425 (6th Cir. 2020)).

201. See, e.g., United States v. DiTomasso, 81 F. Supp. 3d 304, 307–10 (S.D.N.Y. 2015) (concluding that Omegle did not intend its CSAM monitoring to assist law enforcement based on a declaration by the platform's founder that Omegle monitored chats "to improve the user experience by removing inappropriate content" in response to "negative media attention" (citation omitted) (internal quotation marks omitted) (quoting Lief K-Brooks)).

202. See supra notes 61–62 and accompanying text.

203. See, e.g., United States v. Cameron, 699 F.3d 621, 638 (1st Cir. 2012) ("[I]t is certainly the case that combating child pornography is a government interest. However, this does not mean that Yahoo! cannot voluntarily choose to have the same interest."). For these reasons, providers would likely not be considered state actors under the Second Circuit's nexus test either. The nexus test is stricter than the critical factors test used by most other circuits since the "requisite nexus is not shown merely by government approval of or acquiescence in the activity." United States v. DiTomasso, 932 F.3d 58, 68 (2d Cir. 2019). Whether providers would be considered state actors under the compulsion and public forum tests is unclear since the bill does not explicitly compel providers to search for drug-related activity and regulated entities do not clearly perform a public function. Cf. Prager Univ. v. Google LLC, 951 F.3d 991, 996–99 (9th Cir. 2020) (holding that YouTube is not a public forum subject to the First Amendment despite hosting speech by others).

First, courts should not attempt to discern providers' subjective intent given how intertwined platforms' economic and legal interests are.[204] The Supreme Court's decisions have focused more on the actions of the *state* than the private party,[205] and the second prong of the "critical factors" inquiry requires courts to reconstruct providers' subjective intent, often leading to "inconsistent and unpredictable results."[206] Discerning subjective intent is particularly challenging with regard to providers, as companies are rarely acting with a single intent; as profit-driven entities, providers may consider assisting law enforcement to be part and parcel of furthering their business ends.[207]

Economic and legal interests are particularly intertwined under the Cooper Davis Act: Providers may well have an interest in eradicating illegal drug activity from their platforms, but unlike CSAM, which "inherently lacks any redeeming social value,"[208] proscribing suspected drug-related activity may sweep in a broad range of desirable speech, including journalism, research, and public health messages, that providers want to retain.[209] While providers lack any justifiable interest in protecting CSAM, they *do* have a strong business interest in protecting user speech.[210] Courts

---

204. See Jeff Kosseff, Private Computer Searches and the Fourth Amendment, 14 I/S: J.L. & Pol'y for Info. Soc'y 187, 190 (2018) (arguing that "courts should rework their Fourth Amendment agency tests to focus on the objective actions of both the government and private parties, rather than attempting to guess the intent of private parties").

205. See, e.g., Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989) (stating that agency hinges on "the degree of the Government's participation in the private party's activities"); Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971) (stating that attempts by the government to "coerce," "dominate," or "direct" the actions of a private person may result in a search and seizure that implicates the Fourth Amendment).

206. Kosseff, supra note 204, at 206 ("Courts examine whether the private party *intended* to assist law enforcement, or whether the private party intended to advance its own interests that are unrelated to law enforcement. Similarly, courts consider whether the government *knew* of the private party searches.").

207. See id. at 215 (emphasizing that courts struggle to discern providers' motives because providers can "have a number of intentions"—from helping law enforcement to preventing child exploitation to protecting their business interests); see also Avidan Y. Cover, Corporate Avatars and the Erosion of the Populist Fourth Amendment, 100 Iowa L. Rev. 1441, 1445 (2015) (arguing that tech companies have economic and legal incentives to cooperate with government surveillance); Slobogin, supra note 160, at 19 (noting that for businesses, even "volunteered" disclosures are often "driven by the hope of cultivating government favor, in all sorts of ways, ranging from beneficial regulatory decisions to direct sales"); Bruce Schneier, Opinion, Spy Agencies Are Addicted to Corporate Data Load, Bloomberg (July 31, 2013), https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership (on file with the *Columbia Law Review*) (arguing that the "primary business model of the Internet is built on mass surveillance").

208. Bloch-Wehba, Automation in Moderation, supra note 13, at 83.

209. The same is true of hash searches for terrorist and extremist content, which is also context dependent. See supra note 107.

210. This concern may be particularly acute for providers who want to avoid accusations of colluding with the government to censor unpopular speech on their platforms. See, e.g., Murthy v. Missouri, 144 S. Ct. 1972, 1997 (2024) (Alito, J., dissenting) (discussing how federal officials allegedly coerced social media platforms into suppressing user speech in a

adopting an intent-based agency test are likely to reach inconsistent and unpredictable results, making it difficult for providers to determine ex ante whether they are subject to the Fourth Amendment and how to structure their businesses accordingly. This unpredictability poses practical difficulties for providers, many of which already use automated drug-detection tools.[211]

Second, courts must take seriously the notion that state action may be present even in the absence of explicit government compulsion.[212] In *Skinner*, the Court found relevant that the government had "removed all legal barriers to the testing" of employees by private railroad companies and had "made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions."[213] The Court considered these factors "clear indices of the Government's encouragement, endorsement, and participation" sufficient to render the railroads government agents.[214] Similarly, the Cooper Davis Act removes legal barriers that currently limit providers' ability to share the contents of user communications with the government.[215] Like the federal regulations in *Skinner*, the bill makes plain Congress's strong preference for surveillance as well as its desire to share the fruits of such surveillance: The bill imposes severe criminal and civil penalties on providers that turn a blind eye to "readily apparent" drug crimes, and the DEA stands to benefit from direct access to reported evidence.[216]

While courts may still ultimately conclude that providers are private parties under the Cooper Davis Act, an analysis that disregards subjective intent and takes seriously the blindness provision will provide clarity to providers about their obligations under the Fourth Amendment, or lack thereof, and to individuals about their rights in a rapidly changing digital landscape.

"'far-reaching and widespread censorship campaign' . . . against Americans who expressed certain disfavored views about COVID-19 on social media" (quoting Missouri v. Biden, 680 F. Supp. 3d 630, 729 (W.D. La. 2023))). Providers have also faced intense public scrutiny after taking down obviously innocuous content caught by their algorithms. See supra note 108 (discussing Facebook and Tumblr's gaffes).

211. See supra note 106 and accompanying text.

212. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614–15 (1989) ("The fact that the Government has *not* compelled a private party to perform a search does not, by itself, establish that the search is a private one." (emphasis added)).

213. Id. at 615.

214. Id. at 615–16.

215. The Stored Communications Act prohibits providers from divulging the contents of user communications to law enforcement except in limited circumstances. See 18 U.S.C. § 2702(b)(7) (2018) (noting that a provider may divulge the contents of communications to a law enforcement agency if the contents "were inadvertently obtained" and "appear to pertain to the commission of a crime").

216. See Hannah Bloch-Wehba, Content Moderation as Surveillance, 36 Berkeley Tech. L.J. 1297, 1299 (2021) ("As police increasingly depend upon digital evidence in investigating and prosecuting crime, content governance strategies also shape the kinds of data that are germane to investigations and affect how law enforcement does its job.").

C. *Adopting the First-Look Approach to the Private Search Doctrine*

Assuming providers remain private entities under the Cooper Davis Act, the government's ability to rely on private surveillance will turn on the scope of the private search exception. This section argues that courts should adopt the Ninth Circuit's first-look approach and require human review of an automated search before applying the private search exception.

1. *Rejecting the Sui Generis Approach.* — The approach taken by the Fifth and Sixth Circuits is inapposite outside the sui generis world of CSAM hard hashing. First, hash matching depends on the availability of highly reliable systems that can identify CSAM with near-absolute certainty. Hash matching is possible only because providers have access to, or have developed their own, hash databases containing content already vetted by experts trained in the legal definition of CSAM.[217] But no such database exists, or could exist, for drug crimes since the "facts and circumstances" establishing drug crimes are often nonvisual, subjective, and may constitute lawful—even socially beneficial—speech.[218]

Furthermore, the rationale for the sui generis approach—that a hash search frustrates any legitimate expectation of privacy by detecting the presence of contraband—does not apply to detection of drug-related content since such searches are not merely confirmatory but necessarily context dependent.[219] As a result, courts should apply the private search exception only if a human has already viewed the private electronic communications before reporting them to the government.[220] Otherwise, if no private party has viewed the contents of the private communications, the government conducts a new search requiring a warrant.[221]

2. *Benefits of the First-Look Approach.* — The first-look approach comports with the Supreme Court's formulation of the private search doctrine as being premised on private searches conducted by *individuals*,

---

217. See supra notes 80, 95 and accompanying text (discussing Google and AOL's databases).

218. See supra note 209 and accompanying text. Consider, for instance, how lawful speech has been misidentified as "terrorist content." See supra note 107.

219. See supra section II.A. An additional, more practical reason to reject the sui generis approach is that courts should not base their definition of a sweeping Fourth Amendment exception on their perceptions of a cutting-edge algorithm's reliability and accuracy—especially in a rapidly evolving area like machine learning. This would likely lead to forum shopping, as with any circuit split; a doctrine that applies uniformly across the circuits is preferable given that most major providers' services are used nationwide.

220. See supra section I.C.2.

221. For the hypothetical scenario involving Provider B, see supra section I.C, the government would exceed the scope of the private search by viewing messages reported solely based on an algorithm since, no matter how advanced the algorithm, the government would risk exposing more personal information than what the hit alone would convey. See supra note 92 and accompanying text. The government also learns much more information from viewing these messages than it would by viewing a file detected by a hash match.

not machines.[222] In *Walter*, the Court held that the films' owners retained a reasonable expectation of privacy in their films even after employees had opened their packages and exposed the films' labels—the owners "expected no one except the intended recipient either to open the . . . packages or to project the films."[223] The film boxes had been "securely wrapped and sealed, with no labels or markings to indicate the character of their contents," and the employees' opening of the packages to reveal the film boxes constituted a partial invasion of privacy, not a complete one.[224] Similarly, users retain a reasonable expectation of privacy in electronic communications that they expect only their intended recipient to see, and an automated search of such communications, no matter how accurate, does not constitute a complete frustration of an individual's privacy interest.[225]

Such a rule makes intuitive sense: A true "frustration" of privacy requires that a person actually view the private information.[226] Applied to the Cooper Davis Act, this rule is also consistent with the text of the statute—"actual knowledge" requires actual *human* knowledge of suspected illegal activity, and a violation of the statute is only "readily apparent" if a provider has actually viewed the facts or circumstances establishing a drug crime.[227]

3. *Addressing Potential Criticisms.* — Requiring human review to constitute a private search has some drawbacks. Most obviously, it may undermine one of the main benefits of automation: lessening the human toll of content moderation.[228] Still, effective content moderation requires

---

222. Both *Walter* and *Jacobsen* involved private searches by individual employees of suspicious materials. See supra notes 72, 84–86 and accompanying text.

223. Walter v. United States, 447 U.S. 649, 658 (1980).

224. Id. at 658–59.

225. In *Carpenter*, the Supreme Court emphasized that while there is a reduced expectation of privacy in information knowingly shared with others, "the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'" Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (quoting Riley v. California, 573 U.S. 373, 392 (2014)).

226. While the circuits may be divided on how to handle edge cases involving hash matches that were not confirmed by a provider, courts universally agree that the government does not conduct a new search when it views material that a human reviewer has already seen. See supra note 66.

227. See supra note 20 and accompanying text.

228. For accounts of the intense human impact of content moderation, see Andrew Arsht & Daniel Etcovitch, Commentary, The Human Cost of Online Content Moderation, Harv. J.L. & Tech.: JOLT Digest (Mar. 2, 2018), https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation [https://perma.cc/3Z52-DBHH]; Isaac Chotiner, The Underworld of Online Content Moderation, New Yorker (July 5, 2019), https://newyorker.com/news/q-and-a/the-underworld-of-online-content-moderation (on file with the *Columbia Law Review*). Manual review of all automated search results may also be unrealistic and greatly strain providers' resources, limiting the potential efficacy of a law like the Cooper Davis Act. See Stackpole, supra note 113 (noting that without human

a combination of ex ante automated screening *and* ex post human review, and many providers use both before voluntarily disclosing evidence to law enforcement.[229] The proposed approach would therefore be unlikely to substantially change providers' procedures in practice.

While providers are indeed constrained by their capacity to hire content moderators, the proposed approach best balances individuals' privacy interests in the contents of their electronic communications against providers' (and the government's) legitimate goal of preventing harmful activity. Unlike the sui generis approach, this rule provides ex ante clarity to providers, giving them notice of what circumstances trigger the private search exception since the rule applies consistently to different kinds of automated moderation, regardless of what form the technology takes—including fuzzy hash matching.[230]

This approach is also consistent with how individuals expect providers to handle their private data. In their terms of service, many providers alert users of the possibility that they may refer illegal activity to law enforcement, so users reasonably expect that providers sometimes share data with the government to prevent imminent harm.[231] But users do not—and should not—expect these services to operate as surrogates for law enforcement, algorithmically combing through their personal data for evidence of crimes and reporting that evidence without a human at least performing some verification first.[232] A law like the Cooper Davis Act would bring an unprecedented amount of personal information into the hands of law enforcement, regardless of which side of the circuit split prevails.[233] And given the history of overenforcement of drug crimes in

---

content moderators, "social media companies—and their ad-driven business models—likely couldn't exist as they do now").

229. See Bloch-Wehba, Automation in Moderation, supra note 13, at 84. Ex post human review is particularly crucial when it comes to suspected instances of context-dependent crimes, like drug trafficking, so that providers can catch false positives. See supra notes 210, 218 and accompanying text.

230. Some might interpret the first-look approach as requiring manual review of CSAM hash matches as well, which would dramatically hinder the government's ability to fight CSAM. But this rule leaves courts' jurisprudence intact for CSAM hashing, at least for searches conducted via hard hashing. Hard hashing is premised on the fact that at least one private party (either at NCMEC or a provider) has at one point viewed the file and classified it as CSAM, and that initial viewing of the file by a private party satisfies the first-look approach. See supra note 66; supra text accompanying note 162. In contrast, a fuzzy hash match does not guarantee that a flagged file is the same as one that has been vetted by a private party. See supra notes 164–168 and accompanying text.

231. See supra note 185 and accompanying text.

232. See Kerr, Terms of Service, supra note 127, at 325 ("When a person signs up for an account with a private provider, . . . [t]he government's future role is an abstraction. . . . [T]here is a possibility that the government might someday be involved . . . [but] the mere act of proceeding after receiving such an abstract future conditional warning is insufficient to generate consent.").

233. Whether encouraged by law or adopted voluntarily, automated content moderation "open[s] new kinds of behavior and new actors to scrutiny that [were]

communities of color,[234] the bill raises serious concerns about how the government might prosecute drug crimes using the trove of information that providers would be required to report. Against this backdrop, courts must adopt an approach to the private search exception that maintains the status quo and does not risk overburdening users' privacy rights.[235]

CONCLUSION

As more and more illegal activity occurs on the internet—on third-party platforms and out of the government's sight—the government has more and more reasons to outsource surveillance to providers through legislation like the Cooper Davis Act.[236] This Note shows that although the Cooper Davis Act is modeled after the PROTECT Act, analysis of its constitutionality—and, more broadly, of Fourth Amendment issues raised by automated content moderation and mandatory reporting statutes for providers—requires a different approach, as much of the reasoning regarding CSAM is inapplicable outside the narrow realm of hard hashing.

While the Cooper Davis Act's future is uncertain, it poses important Fourth Amendment questions that extend beyond a single piece of legislation and are likely here to stay. Providers rely on rapidly evolving technologies like machine learning and artificial intelligence to detect unwanted content on their platforms, and some state legislatures have introduced legislation similar to the Cooper Davis Act aimed at halting drug activity on social media platforms.[237] Regardless of whether the

---

previously beyond the state's capabilities." Bloch-Wehba, Automation in Moderation, supra note 13, at 80.

234. See generally Drug Pol'y All., The Drug War, Mass Incarceration and Race (2015), https://www.unodc.org/documents/ungass2016/Contributions/Civil/DrugPolicyAlliance/DPA_Fact_Sheet_Drug_War_Mass_Incarceration_and_Race_June2015.pdf [https://perma.cc/98WH-NG8F] (showing how the war on drugs has driven racial disparities in U.S. incarceration); Jay Stanley, The War on Drugs and the Surveillance Society, ACLU (June 6, 2011), https://www.aclu.org/news/smart-justice/war-drugs-and-surveillance-society [https://perma.cc/AZ7N-GZ3N] (describing the role of electronic surveillance in the war on drugs).

235. See Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 482 (2011) (arguing that courts should respond to changing technologies and social practices that expand police power by "tighten[ing] Fourth Amendment rules to restore the status quo").

236. See generally Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (K. Jaishankar ed., 2011) (discussing the prevalence of cybercrimes); Internet Crime Complaint Ctr., FBI, Internet Crime Report 2022, at 3 (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf [https://perma.cc/G2PC-VF63] (noting that "[t]oday's cyber landscape has provided ample opportunities for criminals and adversaries").

237. See, e.g., S.B. 680, 2023 Leg., Reg. Sess. (Cal. 2023) (proposing to ban providers from using features or algorithms that they know, or reasonably should know, will cause harm to children, including receiving information about obtaining a controlled substance and subsequently obtaining or using it); Queenie Wong, California Lawmakers Want to Make Social Media Safer for Young People. Can They Finally Succeed?, L.A. Times (Aug. 9,

Cooper Davis Act is enacted, the constitutionality of mandatory reporting laws and the scope of the private search exception will only become more relevant as automated content moderation methods improve and Congress and the states continue legislating with an eye toward tech companies.[238]

2023), https://www.latimes.com/politics/story/2023-08-09/meta-instagram-twitter-tiktok-social-media-onlinesafety (on file with the *Columbia Law Review*).

238. See supra note 158 (describing Congress's proposed EARN IT and STOP CSAM Acts).