Note

(CTRL + F)OURTH AMENDMENT SEARCHES OF DIGITAL STORAGE DEVICES: A NOVEL FRAMEWORK

JAMES MULLEN†

ABSTRACT

Judges frequently analogize physical precedents when applying Fourth Amendment law to searches of digital storage devices. But these analogies do not map well from physical to digital spaces because they overlook fundamental structures of digital storage. And the stakes are high—courts' errors lead to oversearches that irreparably harm device owners regardless of the suspects' guilt or innocence. This Note examines the structure of common digital storage devices and courts' erroneous attempts to apply Fourth Amendment law to them.

This Note also proposes a novel two-phase framework that would curb oversearch. The framework uses a forensic program to conduct a limited analysis of digital devices to estimate the probability that the device contains the sought-after evidence. Judges then use that probability when weighing the reasonability of a thorough search of the device. By expanding the reasonability determination for the search and seizure of digital devices, this Note's proposed framework would reduce oversearch and improve conformity with traditional Fourth Amendment law.

INTRODUCTION

Despite his clean public image, Matthew Mann lived an insidious double life. His friends and neighbors knew him as a high school teacher and a Red Cross lifeguard instructor in Tippecanoe County,

† Duke University School of Law, J.D. expected 2025; Utah State University, B.S. 2022. I thank Professor Rebecca Rich and my classmates in the Fall 2023 Scholarly Writing Workshop at Duke Law for their insight and feedback. I am and will forever be appreciative to my friends and colleagues on *Duke Law Journal* for the attention, care, and effort they expended on this piece. Finally, I am grateful to Selendra for her unwavering patience and to Jack Bradley, who inspired this topic.

Indiana.[1] But, on a May morning, everything changed.[2] One of Mann's lifeguard students found a hidden video camera inside the women's locker room. The tape only contained a few hours of footage, but it had captured Mann as he placed and disguised the camera.[3] The camera had also recorded footage of several adult female students undressing.[4]

The lifeguard students took the camera to the local police, and a state prosecutor began investigating Mann for voyeurism.[5] The prosecutor sought a warrant, arguing that he had probable cause to search all of Mann's digital storage devices because voyeurs tend to keep stashes of their illegal videos.[6] Based on the evidence presented, the judge issued a warrant permitting officers to search Mann's home for "videotapes, cd's [*sic*] or other digital media, computers, and the contents of said . . . electronic media" to locate evidence of voyeuristic activities.[7] Officers executed the search and seized two computers, multiple hard drives, flash storage, video recorders, video tapes, CDs, and other electronic storage devices.[8] After officers searched his house, Mann confessed to having set up the camera and entered a guilty plea.[9]

At the end of July, weeks after Mann had agreed to the plea deal and months after officers had seized his electronics,[10] an officer began reviewing the contents of Mann's electronic storage devices.[11] The officer, searching the devices out of a desire for "complete[ness],"[12] moved systematically through each storage device and examined them

---

1. *Accused Voyeur Arrested*, WTHR (June 1, 2007, 3:11 PM), https://www.wthr.com/article/news/local/accused-voyeur-arrested/531-5851b341-24fd-4641-b73b-a19b757babb8 [https://perma.cc/XS8N-KTHY].

2. *See* United States v. Mann, No. 2:07-CR-197, 2008 WL 1701743, at *1 (N.D. Ind. Apr. 8, 2008), *aff'd*, 592 F.3d 779 (7th Cir. 2010) (describing Mann's criminal indictment).

3. *Id.*

4. *Id.* at *2.

5. Voyeurism is the crime of "any looking of a clandestine, surreptitious, prying, or secretive nature." IND. CODE § 35-45-4-5(a)–(c) (West 2011).

6. *Mann*, 2008 WL 1701743, at *3–4.

7. *Id.* at *4.

8. *Id.* at *2.

9. *Id.*

10. Justice Sonia Sotomayor wrote in her concurrence in *Jones* that "[t]he government can store [digital] records and efficiently mine them for information[,] . . . evad[ing] the ordinary checks that constrain abusive law enforcement practices." United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring).

11. United States v. Mann, 592 F.3d 779, 781 (7th Cir. 2010).

12. *See Mann*, 2008 WL 1701743, at *2 (noting that the detective did not know Mann had agreed to the guilty plea and that the detective testified that he would have "continue[d] [his] investigation until it was complete" even if he had known about the plea).

with both forensic software tools and manual review techniques.[13] The officer pored through the media for over two months.[14] In some devices, he found nothing pertinent to Mann's criminal activity.[15] In others, he found pictures and videos Mann had recorded in the locker room, which confirmed his voyeurism charge.[16] Then, the officer discovered a cache containing hundreds of child pornography images unrelated to Mann's voyeurism.[17] The prosecutors brought additional charges against Mann for possession of child pornography.[18]

Mann filed a motion to suppress this additional evidence, arguing the detective's search exceeded the scope of the initial warrant.[19] He argued the warrant was constitutionally inadequate because it did not describe the items to be searched with sufficient particularity to prevent a general search of his possessions.[20] A warrant's description must be specific enough to limit the scope of the search to items where officers are likely to find sought-after content.[21] Mann maintained that the officer's search extended past the prescribed limits of the warrant and constituted a "general search" for evidence of crimes unrelated to the crimes charged.[22] The Seventh Circuit disagreed; because there could be digital evidence of Mann's crimes anywhere on his electronic storage, the officer could search through every device.[23]

At first cut, this result seems acceptable. Mann traded child pornography and must answer for his crimes. The investigating officer had a warrant, and his search did not cover that much data. After all,

---

13. *Id.* at *7.

14. *Mann*, 592 F.3d at 781.

15. *Mann*, 2008 WL 1701743, at *3.

16. *Id.*

17. *See Mann*, 592 F.3d at 781 ("Detective Huff uncovered still images taken in the Jefferson High school locker room [and] child pornography . . . .").

18. *See id.* at 781–82 (describing how Mann pleaded guilty to a child pornography charge after his voyeurism charge).

19. *Id.* at 781.

20. *Id.* at 783.

21. Horton v. California, 496 U.S. 128, 139–40 (1990).

22. *Mann*, 592 F.3d at 783.

23. *Id.* at 784. The Court emphasized that it was "troubling" that the detective "faile[d] to stop his search and request a separate warrant for child pornography" and "problematic" that the search occurred two months after the guilty plea. *Id.* at 786. However, because the pornographic images were discovered as part of a "systematic search for evidence of voyeurism," the search fell "within the scope of the warrant's authorization." *Id.*

Mann's hard drives were barely larger than the local storage on a modern smartwatch.[24] However, nagging questions remain about the permissible scope of digital searches, like those in Mann's case.[25] Why could the investigators pore through Mann's digital devices—many of which had no criminal content—before stumbling across one with new evidence?[26] And why could prosecutors use the new evidence to convict Mann if the warrant never authorized investigators to search for and seize evidence of that crime?[27]

Investigators in *Mann* and similar cases can search suspects' devices thoroughly because many courts treat digital devices like any other storage media.[28] Those courts reason that if computers are no different than letters and paper folders, the Fourth Amendment should apply to them in the same way.[29] This thinking not only overlooks the

24. For example, the Apple Watch Series 8's storage is within an order of magnitude of Mann's hard drives. *Compare Apple Watch Series 8 – Technical Specifications*, APPLE (2022), https://support.apple.com/en-us/111848 [https://perma.cc/5L3R-EK7D] (advertising a thirty-two gigabyte capacity), *with Mann*, 2008 WL 1701743, at *3 (listing hard drives with storage between 20 gigabytes and 160 gigabytes).

25. *See infra* Part III (discussing several cases with expansive searches of digital storage).

26. Of course, there is no way to know conclusively that a device does not contain evidence of a crime until investigators search the device. Many devices will not contain anything related to criminal activity. *See* United States v. Ganias, 824 F.3d 199, 217 (2d Cir. 2016) (en banc) ("The seizure of a computer hard drive . . . can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure."). However, investigators should have a minimum degree of certainty that their search will be successful before starting. *See* United States v. Griffith, 867 F.3d 1265, 1274 (D.C. Cir. 2017) ("Because a [computer], unlike drugs or other contraband, is not inherently illegal, there must be reason to believe *that* a [computer] may contain evidence of the crime." (emphasis added)).

27. *See* Commonwealth v. Yusuf, 173 N.E.3d 378, 392 (Mass. 2021) ("[P]rivacy rights . . . must be preserved and protected as new technologies are adopted" because permitting officers to "trawl through" digital storage looking for "evidence of crimes unrelated to the officers' lawful [intrusion] . . . is the virtual equivalent of a general warrant." (citations omitted)).

28. Stephen Moccia, *Bits, Bytes, and Constitutional Rights: Navigating Digital Data and the Fourth Amendment*, 46 FORDHAM URB. L.J. 162, 165 (2019); *see also id.* at n.13 (listing five examples of courts using physical analogies instead of grappling with digital storage directly).

29. *Id.* at 165.

differences between digital and physical media,[30] but also ignores the reality of digital evidence collection.[31]

Two centuries of Fourth Amendment precedent developed to regulate searches of physical property, documents, and homes is ill-equipped to handle the complexities courts face in cases where evidence is stored digitally.[32] Courts struggle to apply the traditional Fourth Amendment theories, analogies, and tests to modern investigative procedures.[33] Legal rules do not translate well from physical property to digital information.[34] Ambiguity in courts' strained analogies leads to the overseizure of information.[35]

Mann and similar cases demonstrate how courts' refusal to adjust warrant requirements for electronic storage erodes fundamental

30. *See* Riley v. California, 573 U.S. 373, 393–95 (2014) (distinguishing evidence stored on smart phones from physical evidence). Saying the search of data on a digital storage device is "'materially indistinguishable' from searches of . . . physical items . . . is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 393. Furthermore, the storage capacity of digital devices has interrelated implications for privacy, including additional context from the combination of "many distinct types of information" in one location; information-rich files "convey[ing] far more than previously possible"; the retention of data dating back "to the purchase of the [device], or even earlier"; and an inherent "element of pervasiveness that characterizes [digital storage] but not physical records." *Id.* at 394–95.

31. *See infra* notes 77–96 and accompanying text for a discussion of how courts have begun to apply Fourth Amendment precedents differently to electronic devices in certain circumstances.

32. Kelsey Joy Smith, Note, *The Constitutional Right to Deletion: The Latest Battle in the War of Technology v. Privacy*, 42 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 121, 122 (2016); Nathan Freed Wessler, *The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In*, ACLU (June 28, 2019), https://www.aclu.org/news/privacy-technology/supreme-courts-most-consequential-ruling-privacy-digital [https://perma.cc/H95H-DW7L] ("The quantities and types of information that might be discovered by a manual search of a car's trunk and glove compartment . . . pale in comparison to the kinds of comprehensive data stored on our electronic devices today. This requires greater protections under the Fourth Amendment.").

33. United States v. Ganias, 755 F.3d 125, 134 (2d Cir. 2014) ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting) (noting that as "[s]ubtler and more far-reaching means of invading privacy . . . become available," it is the Court's obligation to prevent the "progress of science" from eroding Fourth Amendment guarantees).

34. *See* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 132 (2011) ("The difficulty applying—indeed, even enunciating—what these rules mean . . . suggests that these rules cannot sensibly be 'translated' at all.").

35. Smith, *supra* note 32, at 140; Wessler, *supra* note 32 ("[O]ld-world rules can't be twisted into unfettered authority to search the incredible volumes of data on people's [computers] . . . .").

constitutional rights.[36] Like international expert Sarah St. Vincent has observed, although "[t]hese defendants are not very popular, [] a dangerous precedent is a dangerous precedent that affects everyone."[37] Many of the reported cybercrime cases where courts have not limited the scope of digital searches have resulted in the discovery of child pornography.[38] But people who possess illicit content are not the only ones subject to excessive searches—there could be countless innocent people incorrectly suspected of crimes whose digital devices are similarly searched whose stories will never appear in a court reporter.

The Fourth Amendment stands to protect not only innocent people but also those guilty of crimes from unjustifiable privacy intrusions. The worrisome precedent from *Mann* harms anyone subject to an investigation because it authorizes an unconstrained search of suspects' devices, regardless of the probability the devices contain any evidence whatsoever related to alleged criminal activity.[39]

Thus, courts should implement a new framework to govern the search and seizure of private digital storage devices. To prevent the

---

36. United States v. Ulbricht, 858 F.3d 71, 99 (2d Cir. 2017) ("A general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be 'akin to a residence in terms of the scope and quantity of private information [they] may contain.'").

37. Jack Gillum, *Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned*, PROPUBLICA (Apr. 3, 2019, 5:00 AM), https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned [https://perma.cc/7YWM-HNSV].

38. *See, e.g.*, United States v. Mann, 592 F.3d 779, 781 (7th Cir. 2010) (finding child pornography during an authorized search for evidence of voyeurism on a computer); United States v. Crist, 627 F. Supp. 2d 575, 577–78 (M.D. Pa. 2008) (finding child pornography in a warrantless forensic examination of a computer); *cf.* United States v. Ganias, 824 F.3d 199, 206–07 (2d Cir. 2016) (finding evidence of individual tax fraud during an authorized search for evidence of company tax fraud on a hard drive). Some sources estimate that half of all computer crimes involve child exploitation. Robyn Burrows, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 GEO. MASON L. REV. 255, 257 (2011). Cases with child pornography might also appear frequently among cases with searches of unlimited scope because of the high proportion of child pornography cases prosecuted generally. For example, in Pennsylvania, 68 percent of prosecuted cybercrimes between 2014 and 2018 were child pornography offenses. *Pennsylvania Cybercrime–By the Numbers*, UNIFIED JUST. SYS. PA., https://www.pacourts.us/news-and-statistics/news/news-detail/1010/pennsylvania-cybercrime%E2%80%94-by-the-numbers [https://perma.cc/9EPH-TVSR].

39. A computer "is likely to contain . . . non-contraband information of exceptional value to its owner." United States v. Mitchell, 565 F.3d 1347, 1351 (11th Cir. 2009). But "the exposure of confidential and personal information has permanence. It cannot be undone. Accordingly, the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (en banc).

search of devices unlikely to contain evidence of criminal activity, this Note proposes a framework that outlines search procedures, suggests an innovative two-phase warrant approach, and utilizes a theoretical digital forensics program.

The framework defines digital evidence at the file level[40] and utilizes a two-phase warrant and a hypothetical forensics tool to prevent the search of devices without evidence. In Phase One, officers demonstrate probable cause to a judge by showing that an individual may possess incriminating digital evidence. A warrant authorizes the officers to seize the devices and use a forensics program—a program this Note calls "ImperfectTool"—to perform a limited analysis. ImperfectTool estimates the probability that the device does, in fact, possess the sought-after evidence. Then, in Phase Two, the judge decides whether to authorize a comprehensive search of the device by considering ImperfectTool's probability together with the traditional Fourth Amendment reasonableness balancing test.

This Note's framework better preserves suspects' privacy, increases officers' efficiency, facilitates judges' reasonableness determinations, and conforms with tangible search and seizure analogs. This Note proceeds in four parts. Part I sketches a background of Fourth Amendment applications in criminal investigations. Part II describes the most common methods of modern electronic data storage and other important characteristics of computer systems. Part III identifies how courts have erred mapping real-world precedents onto digital Fourth Amendment law. Part IV outlines a unified framework that combines a file-based method to conceptualize digital data, a novel two-phase warrant requirement, and a theoretical forensic tool to better protect Fourth Amendment rights in the digital age. Part IV further demonstrates how the framework simplifies controversial criminal cases and better protects individuals' fundamental rights "to be secure in their persons . . . and effects, against unreasonable searches and seizures."[41]

40. *See infra* Part III.B.3 (describing the subcontainer approach used to isolate individual units of evidence).

41. U.S. CONST. amend. IV.

I. SETTING THE (CRIME) SCENE: FOURTH AMENDMENT BACKGROUND

Fourth Amendment protections are older than the nation itself.[42] The Founders incorporated the Fourth Amendment into the Bill of Rights to prevent the use of writs of assistance, which empowered British officials to conduct dragnet searches and collect evidence of any crime in the colonial era.[43] The Fourth Amendment mandates that every search, even those conducted with a warrant, be reasonable.[44] Modern privacy protections rely on these same principles.[45]

For two centuries, courts have developed case law circumscribing the Fourth Amendment's scope and outlining its limited exceptions.[46] A valid warrant rests upon two pillars: probable cause and specificity.[47] And a warrantless search is presumptively unreasonable if the action violates a person's expectation of privacy[48] or common-law property rights.[49]

First, warrants require sufficient probable cause to motivate the search or seizure.[50] Probable cause does not mean concrete evidence of the subject's guilt.[51] Rather, an officer must produce "more than [a] bare suspicion"[52] or a "strong reason to suspect"[53] that the subject

---

42. Signatories of the Articles of Confederation had protections against excessive searches and seizures in their declarations of rights. *See* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 79–80 (1937).

43. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005) [hereinafter Kerr, *Searches and Seizures*].

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

45. Kyllo v. United States, 533 U.S. 27, 34 (2001) (noting that modern protections should "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").

46. *See generally* Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry*, 72 MINN. L. REV. 383, 386–97 (1988) (discussing the two requirements).

47. The Honorable Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 799 (2004); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 558 n.12, 577 n.67 (1999).

48. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

49. United States v. Jones, 565 U.S. 400, 405–07 (2012).

50. Gould & Stern, *supra* note 47, at 785–86 (describing the probable cause requirement).

51. *See* Spinelli v. United States, 393 U.S. 410, 419 (1969) (citing Beck v. Ohio, 379 U.S. 89, 96 (1964)).

52. Brinegar v. United States, 338 U.S. 160, 175 (1949).

53. Henry v. United States, 361 U.S. 98, 101 (1959) (quoting Conner v. Commonwealth, 3 Binn. (Pa.) 38, 43 (1810)).

engaged in illegal conduct. Second, warrants must also describe with particularity the items the officers will search and seize.[54] The specificity requirement ensures the items officers find and take from a suspect relate to the suspected criminal activity in the warrant application,[55] preventing a descent back to general writs of assistance.

However, the case law is not well suited to address the complexities of digital information.[56] Legal rules do not map well from physical "effects" onto digital information. The ambiguity created by courts' analogies, compounded by the vast quantity of intermingled data on digital storage devices,[57] has led to the overseizure of sensitive information.[58]

Some courts are aware of this problem. In 2008, Justice Nancy E. Rice of the Supreme Court of Colorado noted that digital storage devices hold vast amounts of personal and confidential information.[59] Judge Andrew J. Kleinfeld of the Ninth Circuit went so far as to assert that "for most people, their computers are their most private spaces."[60] These decisions came around a year before the release of the iPhone, when computers were *merely* "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, [and] virtual diaries."[61] Their words ring all the more true now that people generate and store orders of magnitude more data on digital devices.[62] Personal digital storage now contains everything about its user: who the user associates with; where the user

54. Burrows, *supra* note 38, at 266.

55. *See Search and Seizure in the Supreme Court: Shadows on the Fourth Amendment*, 28 U. CHI. L. REV. 664, 687 (1961) (stating that these are "conclusions necessary to the issuance of the warrant" that "must be supported by substantial evidence"—in other words, probable cause).

56. Smith, *supra* note 32, at 122.

57. United States v. Ganias, 755 F.3d 125, 135 (2d Cir. 2014).

58. Smith, *supra* note 32, at 122.

59. Cantrell v. Cameron, 195 P.3d 659, 661 (Colo. 2008).

60. United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting).

61. Kerr, *Searches and Seizures*, *supra* note 43, at 569.

62. *See* Carpenter v. United States, 585 U.S. 296, 312 (2018) (describing how access to computers gives investigators a window into "categor[ies] of information otherwise unknowable" through traditional investigative techniques); *see also* United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) ("The express listing of papers [in the Fourth Amendment] 'reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government.'") (quoting United States v. Seljan, 547 F.3d 993, 1014 (9th Cir. 2008) (en banc) (Kozinski, C. J., dissenting)).

has been; what the user likes, wonders, and wants; and how the user interacts with others.[63] Digital storage is more than "a repository for private information";[64] it is an extension of the self[65] that "provide[s] . . . 'an intimate window into a person's life.'"[66] Privacy provides "sheltering zones for individual liberty, autonomy, seclusion, and self-definition" and is essential for developing "free expression[,] . . . relationships[,] and [] physical and moral space and security."[67]

To grant a warrant, a judge must determine if the need to search outweighs its invasion of privacy.[68] Naturally, this inquiry is fact intensive and fluid; it depends upon the probability that incriminating evidence will be found in a given circumstance.[69] It is thus difficult to create a clear rule to indicate when there is *enough* probable cause to justify a search.[70] Because digital devices contain so much sensitive

63. *See, e.g.*, Robert de Haan, *What is Stored on Your Computer and Mobile Device?*, LAYER 8 SEC. (May 29, 2020), https://layer8security.com.au/what-is-stored-on-your-computer-and-mobile-device [https://perma.cc/H4S7-Y9MT] (listing types of data that contain personal details and are stored on mobile devices and computers).

64. United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007).

65. *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (noting that email is "[an] essential means or necessary instrument[] for self-expression, even self-identification" (internal quotation omitted)); Chang Sup Park & Barbara K. Kaye, *Smartphone and Self-Extension: Functionally, Anthropomorphically, and Ontologically Extending Self via the Smartphone*, 7 MOBILE MEDIA & COMMC'N 215, 215–27 (2019) (exploring the "blurring boundary between the 'human self' and the smartphone" through interviews with sixty smartphone users); Karina Vold, *Is Your Smartphone an Extension of Your Mind?*, VICE (Mar. 2, 2018, 10:00 AM), https://www.vice.com/en/article/qvemgb/is-your-smartphone-an-extension-of-your-mind [https://perma.cc/HB39-ZWJ9] ("If our minds now encompass our phones, we are essentially cyborgs: part-biology, part-technology.").

66. *See* United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020) (attributing these characteristics to digital storage and not to digital services like cryptocurrency transactions).

67. *See* Cameron F. Kerry & John B. Morris, *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS (Dec. 8, 2022), https://www.brookings.edu/articles/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation [https://perma.cc/G8CS-9DBT] (describing "[t]he legal, moral, and historical foundations of privacy in America").

68. Camara v. Mun. Ct. of the City and Cnty. of S.F., 387 U.S. 523, 536–37 (1967).

69. Illinois v. Gates, 462 U.S. 213, 232 (1983).

70. *Id.*

information,[71] reasonableness demands an elevated standard of probable cause to justify the search of a digital storage device.[72]

Some courts and scholars already treat digital information differently than physical items in certain circumstances.[73] It is how digital devices store information[74]—not merely the amount of information they store[75]—that necessitates this differential treatment. To justify the disparate treatment of digital media, courts have relied on individual reasonableness determinations "account[ing] for differences in [the] property."[76]

Federal and state courts have applied Fourth Amendment protections differently to digital property than traditional storage media in at least four scenarios: when seizing cell phones, when specifying which devices officers may remove, when severing seizure warrants from search warrants, and when securing evidence from suspects' residences. In each scenario, Fourth Amendment reasonableness requires different treatment of digital devices.

---

71. Information stored digitally is not merely different in quantity from information stored in the residences of colonial Americans—it is fundamentally different in kind. Much of the health, personal identification, and location information that people store in computers was not even collectable when the Founders penned the Constitution. Perhaps even they would have hesitated to authorize such broad warrants if they had similar information inside their desk drawers.

72. *See* Berger v. New York, 388 U.S. 41, 69 (1967) (Stewart, J., concurring) (stating that, for audio surveillance of an office, "[t]he standard of reasonableness embodied in the Fourth Amendment demands that the showing of justification match the degree of intrusion" and that "[o]nly the most precise and rigorous standard of probable cause should justify an intrusion of this sort"). The misconduct allegations that motivated the surveillance "might be enough to satisfy the standards of the Fourth Amendment for a *conventional* search" but were "constitutionally insufficient to constitute probable cause to justify an intrusion of the *scope* and *duration*" the investigators engaged in. *See id.* at 70 (Black, J., dissenting) (emphasis added).

73. *See* discussion *infra* Part III.

74. *See supra* note 30 (quoting from Riley v. California, 573 U.S. 373, 394–95 (2014)).

75. People v. Diaz, 244 P.3d 501, 508–09 (Cal. 2011) (asserting that a quantitative approach to identify when a heightened standard is necessary would not work because it "would create difficult line-drawing problems for both courts and police officers in the field" and that courts should instead seek a "straightforward, easily applied, and predictably enforced rule . . . [that is not] contrary to [Supreme] [C]ourt precedents" (internal quotations omitted)).

76. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (en banc); *see also Riley*, 573 U.S. at 393 (rejecting the argument that cell phone searches are "materially indistinguishable" from searches of physical items); Carpenter v. United States, 585 U.S. 296, 305 (2018) ("[W]hile the general rule allowing warrantless searches incident to arrest strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to the vast store of *sensitive* information on a cell phone." (emphasis added) (internal quotation omitted)).

Accordingly, this Note's proposal aligns with the broader landscape of modern search and seizure doctrine.

First, the Supreme Court carved out exceptions for cell phones in Fourth Amendment rules. For example, the search incident to arrest rule permits officers to search arrestees and their possessions at the time of arrest.[77] This rule enables officers to secure potential weapons and prevent evidence destruction.[78] The rule is generally not subject to a case-by-case determination. Officers may conduct the search whether or not they—or an objectively reasonable person—believe arrestees have a weapon or evidence on their person.[79] However, officers must obtain a separate warrant before searching the contents of cell phones incident to arrest.[80] The Court's holding recognizes that the search of digital storage requires a heightened level of probable cause beyond that which officers may presume incident to an arrest.[81]

The Court doubled down on its differential treatment of cell phones four years later in *Carpenter v. United States*.[82] There, the Court carved out another exception for cell phones in the third-party doctrine. Typically, suspects lose all expectations of privacy to information they voluntarily give to nongovernment parties.[83] However, cell phone information held by cell service providers—which would fall under a literal application of the third-party doctrine—is exempt from the traditional rule because information from cell phones "present[s] even greater privacy concerns" than evidence obtained through traditional, physical search techniques.[84]

Second, some jurisdictions apply the plain view exception—which permits officers to use evidence of disparate crimes discovered during

77. *Riley*, 573 U.S. at 382–83.

78. Chimel v. California, 395 U.S. 752, 762–63 (1969).

79. *See* United States v. Robinson, 414 U.S. 218, 235–36 (1973).

80. *Riley*, 573 U.S. at 386 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*. We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.").

81. *See Robinson*, 414 U.S. at 235 (holding that a "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification"). Thus, if *Robinson* does not apply to digital media searches, then warrants authorizing the digital media searches require heightened probable cause.

82. *See* Carpenter v. United States, 585 U.S. 296, 306, 309–10, 320 (2018) (declining to extend the Court's third-party doctrine for Fourth Amendment searches to cell phone location records).

83. For more on the third-party doctrine, see *United States v. White*, 401 U.S. 745 (1971).

84. *Carpenter*, 585 U.S. at 311.

a lawful search for new prosecution[85]—differently to digital media than to physical media.[86] Several states do not apply the plain view exception to electronic devices at all.[87] In Oregon, for example, warrants must identify the specific information or data that investigators hope to find on a digital device.[88] The state may not use any other evidence found during the search if it was not specified in the warrant, even if they otherwise could under the plain view exception if the evidence was in physical form.[89]

Third, Washington state requires investigators to obtain separate warrants for the seizure and subsequent searches of digital storage.[90] In federal jurisdictions, authorization to search and seize a piece of physical evidence implies the authorization to search and seize the information contained in that piece of evidence.[91] For example, authorization to seize a particular paper implies the authorization to read the paper. However, in Washington, investigators cannot infer authorization to search the contents of a digital device just because they can seize the device.[92]

---

85. *See infra* notes 181–94 and accompanying text (explaining the plain view exception).

86. *See infra* Part III.B (examining applications of the plain view exception to digital evidence).

87. Oregon is one of many jurisdictions with a heightened specificity requirement to search electronic devices. *See, e.g.*, Price v. State, 119 N.E.3d 212, 224 (Ind. Ct. App. 2019) ("As to what is to be taken, *nothing* is left to the discretion of the officer executing the warrant." (emphasis added) (quoting Marron v. United States, 275 U.S. 192, 198 (1927))); Taylor v. State, 260 A.3d 602, 613–14 (Del. 2021) ("[A] warrant must describe the items to be searched for and seized with as much particularity as the circumstances reasonably allow." (internal quotations omitted)); Wheeler v. State, 135 A.3d 282, 304 (Del. 2016) ("The Ohio Supreme Court [has] recognized that the Fourth Amendment does prohibit a sweeping comprehensive search of a computer's hard drive. . . . [T]he searcher [must] narrow his or her search to only the items to be seized." (internal quotations omitted)).

88. State v. Mansor, 421 P.3d 323, 326 (Or. 2018).

89. State v. Turay, 532 P.3d 57, 69 (Or. 2023).

90. *See* ORIN S. KERR, COMPUTER CRIME LAW, 618 (5th ed. 2021) (citing State v. Fairley, 457 P.3d 1150, 1154 (Wash. App. 2020)) (listing the above as "an example of [the various] approach[es]").

91. This approach is a straightforward application of the plain view exception. *See* South Dakota v. Opperman, 428 U.S. 364, 369–71 (1976) (explaining that when investigators seize a container, they are generally permitted to inventory its contents).

92. *Id.* ("To hold that authorization to search the contents of a cell phone can be inferred from a warrant authorizing a seizure of the phone would be to eliminate the particularity requirement and to condone a general warrant. This outcome is constitutionally unacceptable.").

Fourth, the Ninth Circuit has implemented rules for physical searches that do not apply during search and seizure of digital storage. The circuit does not approve warrants permitting investigators to enter a residence and indiscriminately remove items for future examination in the hopes of discovering evidence of a crime.[93] Instead, investigators must conduct "onsite search and isolation" of potential evidence before taking possession of the suspect's belongings.[94] Investigators may remove the suspect's items only if there is a reasonable suspicion that the items contain evidence of a crime and must leave any item unlikely to contain potential evidence.[95] However, the Ninth Circuit has carved out an exception for digital evidence, which officers can remove without completing the onsite determination and isolation procedure.[96] Although the Ninth Circuit's rule effectively imposes a lower standard for digital evidence, it nonetheless shows the court's willingness to treat physical and digital evidence differently.

However, none of these existing frameworks would have changed anything in cases like Mann's. Investigators can still search computers and storage devices, including devices that contain no evidence of suspects' alleged crimes. And even if officers could not use evidence of other crimes for separate prosecutions, existing accommodations do not protect innocent parties' information from oversearch.[97] But, because both federal and state courts already apply the Fourth Amendment differently to digital and physical storage media, a new comprehensive framework addressing these issues and standardizing such differential treatment would not require a great departure from existing case law.

---

93. United States v. Hill, 459 F.3d 966, 976 (9th Cir. 2006); *see id.* at 975 (describing blanket removal as "seiz[ing] the haystack to look for the needle," an impermissible practice without a "threshold showing" that the search "is reasonable in the case" (internal quotation omitted)).

94. *See id.* at 975–76 (describing the general onsite determination and isolation procedure).

95. *Id.* ("We do not approve of . . . blanket removal of all computer storage media for later examination when there is no . . . reasonable explanation . . . as to why a wholesale seizure is necessary.").

96. *See id.* at 966, 976–78 (holding that even though the warrant "was overbroad in authorizing a blanket seizure" of the defendant's digital media without an onsite determination, evaluating digital media at the crime scene raises practical, logistical, and privacy concerns not implicated during a search of physical storage, which displaces the requirement that officers make a showing of suspicion for each item seized).

97. *See supra* note 39 (describing the permanent and lasting impact of non-contraband data exposure).

II. REBOOT REQUIRED: COMPUTER BASICS

At the most abstract, modern computers are tools that take three steps to complete a task: computers receive commands ("inputs") from a user, perform operations according to the inputs, and store or display the results of those operations ("outputs").[98] However, computers complete tasks quickly, and investigators rarely catch digital criminals in the act.[99] So investigators are forced to search for evidence of previous computer operations—like looking for the "footprints" left when the computer performs processes.[100] Computers deposit this evidence in their storage.

Judges have attempted to use strict formalism when mapping Fourth Amendment precedents onto digital devices to determine when it is permissible for investigators to search for evidence in a computer's storage. They apply rules by analogizing historical cases that address physical storage media to cases that turn on the way people interact with computers.[101] These attempts are clumsy when courts misunderstand the technology.[102] If the judge does not understand how the technology functions, any analogy will be flawed because it will not account for aspects of digital storage that defeat the analogy.[103] Thus, a working knowledge of computer functionality is necessary to develop an enduring framework for digital Fourth Amendment search and seizure doctrine. This Part describes the two types of storage available

98. CONNIE MORRISON, DOLORES WELLS & LISA RUFFOLO, COMPUTER LITERACY 5 (5th ed. 2015).

99. *See* ENHANCEMENT OF PRIVACY AND PUBLIC SAFETY IN CYBERSECURITY ACT, CTR. FOR DEMOCRACY & TECH. 29, https://cdt.org/wp-content/uploads/security/000801cybercrime.pdf [https://perma.cc/UM9J-3A2T] (describing the impediments officers face when investigating suspects' ongoing digital criminal activity); EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 385–86 (3d ed. 2011) (listing the "problem[s] with continued observation" of cybercriminals); Sarah Coble, *How Cybercrime Has Changed Criminal Investigations*, INFOSECURITY MAG. (May 26, 2020), https://www.infosecurity-magazine.com/magazine-features/cybercrime-criminal-investigations [https://perma.cc/R985-WM89] ("It is difficult to place a suspect behind the keyboard . . . . The speed at which cybercrimes and cyber-enabled crimes are committed makes it hard to catch criminals red-handed." (internal quotation omitted)).

100. Unlike the platter analogy, see *infra* notes 241–47, the footprint analogy accounts for the realities of digital storage. Like footprints left in the sand when someone walks on a beach, computers leave evidence when they perform processes. And like footprints, which are washed away by a rising tide, computer evidence is susceptible to being overwritten.

101. *See infra* Part III.

102. *See infra* Part III (highlighting several examples of faulty analogies).

103. For an example of a failed analogy, see *infra* notes 241–47 and accompanying text.

on modern computers and illustrates aspects of computers' operation necessary to understand courts' misapplications of Fourth Amendment precedent.

A. Preserving Information Digitally: How Computers Store Memory

The three steps computers take to complete tasks—receive inputs, perform operations, and output results—are discrete, sequential actions.[104] In reality, computer instructions require many cycles of these steps, and each cycle requires and produces a lot of information.[105] Computers store the information by saving it in digital storage devices.[106]

Computers store information by writing strings of binary code (ones and zeroes)[107] into storage media. Computers need long- and short-term storage to operate effectively.[108] Long-term storage operates slowly but can hold a lot of information.[109] Short-term storage is much faster but can only hold a limited amount of information.[110] One could think of long-term storage like file cabinets and short-term storage like a tabletop. You place papers in the file cabinet to hold them long term, and it takes a long time to open the drawers and locate any particular paper. You place papers that you need to access immediately on a tabletop; it is easy to retrieve and read them, but you can only set so many papers there before the tabletop fills up.

The difference between long- and short-term memory is important to the legal system because the devices could contain different types of

104. MORRISON ET AL., *supra* note 98, at 5–6.

105. *See* SHUANGBAO PAUL WANG, COMPUTER ARCHITECTURE AND ORGANIZATION 51, 54 (2021) (discussing the large amount of storage needed for the products of computer operation); *see also* Jim Young, *Originally Answered: Why Does a Computer Require Storage?*, QUORA (May 21, 2018), https://www.quora.com/Why-does-a-computer-require-storage [https://perma.cc/N57E-WSXM] (providing the example of a computer calculating the sum 1 + 1: The computer needs to recognize that the variable "1" is an integer, understand what the "+" operation does, know how integer-type variables could add together, expect the correct type of result, carry out the operation, and then convert the output into the number two, all of which "use[s] storage[] of various types and characteristics").

106. WANG, *supra* note 105, at 6.

107. *See id.* at 23. That is, consumer computers operate in binary. *Id.* Quantum computers take advantage of quantum states, which possess more than two options. *Id.* at 23, 205. Given the rarity of quantum computers, *id.* at 316, however, the devices are outside the scope of this Note.

108. Jeff Shepard, *Memory Basics – Volatile, Non-Volatile and Persistent*, MICROCONTROLLERTIPS (Aug. 6, 2020), https://www.microcontrollertips.com/memory-basics-volatile-non-volatile-persistent-faq [https://perma.cc/Q2RL-4SYD].

109. *See id.* (discussing long-term memory that is relatively slow but has larger capacity).

110. *Id.*

criminal evidence. People also interact with the devices in different ways, so analogies that make sense for one type of memory break down for the other. Understanding how both long- and short-term memory devices work is the key to understanding why courts' Fourth Amendment analogies are failing.

1. Long-Term Memory. Computers use long-term memory to store information they need for future processes. Long-term memory also stores the user's files and programs. Until recently, the most common consumer long-term digital storage option was magnetic memory devices, like mechanical hard drives. Now, flash memory devices such as solid-state drives are becoming an increasingly popular long-term storage option.[111]

Magnetic memory devices use magnetism to store digital information on disks with a metallic coating.[112] The computer divides the disk into billions of areas, each of which can be individually magnetized. [113] The computer interprets each area as a unit of information, where the magnetization state of an individual area represents either a binary one or zero.[114]

A magnetic memory device works like a record player. When a computer accesses information, the disk spins like a record. An arm moves across the disk and positions a magnet, called the "read/write head," like a record player's needle, over the region on the disk where the desired information is stored. The read/write head senses when the disk areas spinning under it are magnetized and converts that information into a string of ones and zeros.[115]

When a computer stores information on magnetic memory devices, the computer spins up the disk, and the actuator moves the read/write head to the region on the disk where the computer will store

111. *See generally* Yuhui Deng & Jipeng Zhou, *Architectures and Optimization Methods of Flash Memory Based Storage Systems*, 57 J. SYS. ARCHITECTURE 214, 214 (2011) (highlighting the anticipated demand for flash memory); Benj Edwards, *Evolution of the Solid-State Drive*, PCWORLD (Jan. 17, 2012, 6:00 PM), https://www.pcworld.com/article/472983/evolution-of-the-solid-state-drive.html [https://perma.cc/4TKR-7QEV] (identifying flash memory as the "primary storage component in some consumer PCs").

112. E. BALAGURUSAMY, FUNDAMENTALS OF COMPUTERS 52 (2009).

113. *See* MORRISON ET AL., *supra* note 98, at 128, 153 (noting drive magnetization and capacity).

114. PETER NORTON, INTRODUCTION TO COMPUTERS 167 (6th ed. 2008).

115. *Id.*

the information.[116] As the disk spins under the head, a current magnetizes and demagnetizes the head.[117] The head's polarity, in turn, magnetizes or demagnetizes the areas of the disk, writing the information onto the disk through the pattern of the areas' magnetic polarization.[118]

Advanced magnetic memory drives utilize parallel disks attached to the same axle and multiple arms attached to the same actuator.[119] A drive with n disks has a read/write head for each of its $2n$ "platters," the top and bottom surfaces of the n disks.[120] The drive writes a portion of a single collection of information onto parallel clusters on each platter so that, as the disk spins, the parallel read/write heads work simultaneously to access the entire collection.[121]

Because these devices use magnetism to store information, they are nonvolatile, meaning the devices preserve information even if the computer powers off.[122] However, these devices tend to be relatively fragile because they rely on moving components making precise movements.[123] Once the most common form of digital storage, magnetic memory devices are losing popularity to flash memory, a less fragile method of long-term storage.[124]

Flash memory is used in consumer devices such as solid-state drives, multimedia chips, and jump drives.[125] Flash memory is composed of billions of units called floating-gate transistors.[126] Each transistor is like a cup that can trap and hold an electron. The computer uses the charge of trapped electrons to know whether an individual

116. *Id.*

117. *Id.*

118. *Id.*

119. *See id.* at 173 (describing a then-modern hard drive).

120. MORRISON ET AL., *supra* note 98, at 154; *see* Marshall Brain, *What is a Hard Drive and How Does it Work?*, HOWSTUFFWORKS, https://computer.howstuffworks.com/hard-disk.htm [https://perma.cc/CV3F-5LH2] (stating a drive with "three disk platters" has "six read/write heads"); ROBERT F. HOUGHTON, JACK BRADLEY & FALLON DEATHERAGE-BRADLEY, BITS AND BYTES: MASTERING DIGITAL INFORMATION LITERACY 56 (1st ed. 2024).

121. MORRISON ET AL., *supra* note 98, at 154.

122. Shepard, *supra* note 108.

123. Seth Porges, *6 Things You Need To Know About Your Hard Drive*, POPULAR MECHS. (Sept. 18, 2012), https://www.popularmechanics.com/technology/a11912/6-things-you-need-to-know-about-your-hard-drive-12823991 [https://perma.cc/2AXZ-BMGD].

124. Edwards, *supra* note 111.

125. *See* WANG, *supra* note 105, at 54; Chiradeep BasuMallick, *What Is Flash Memory? Types, Working, Benefits and Challenges*, SPICE WORKS (Feb. 22, 2023), https://www.spiceworks.com/tech/hardware/articles/what-is-flash-memory [https://perma.cc/SHY7-FAG3].

126. BALAGURUSAMY, *supra* note 112, at 49–50, 56–57.

floating-gate transistor is "full" or "empty" and translates its state to a binary zero or one. Like magnetic storage, flash memory is nonvolatile and stores its information even when its computer is powered off.[127] However, unlike magnetic storage, which relies on the precise movement of physical architecture, flash memory storage devices tend to be light, durable, and space efficient[128]—a flash device can store many times more information than a magnetic memory device of the same physical size.

Both flash and magnetic memory store information, which can include evidence of computer crimes. However, because flash memory is supplanting magnetic storage, people are storing more material for longer. These growing private historical records increase the need to define how investigators should access and interact with individuals' information.

2. Short-Term Memory. Computers can only perform one operation at a time, so they need some form of storage where they can set information from a completed task and pick up information for their next task. If computers' storage is not fast enough while executing an instruction, tasks that require billions or even trillions of operations would be impractical.[129] So computers use dynamic memory, a form of short-term storage, to hold the information necessary to perform their instructions and information produced by their processes.[130] Most consumer dynamic memory takes the form of random-access memory ("RAM").

RAM is difficult to conceptualize because computer users do not interact with it directly. Information on RAM is not organized in distinct "files," and users typically cannot access it.[131] But this information can still provide investigators with important clues about crimes committed on the computer. For example, information stored on RAM shows what the computer user was last doing when investigators seized the computer[132]—a record of a guilty suspect's red

127. *Id.* at 56; WANG, *supra* note 105, at 54.

128. BALAGURUSAMY, *supra* note 112, at 57.

129. *See What Is Computer and Laptop RAM?*, INTEL CORP., https://www.intel.com/content/www/us/en/tech-tips-and-tricks/computer-ram.html [https://perma.cc/ACD2-MU5Q] (discussing the need for RAM to reduce user wait time).

130. *Id.*

131. Hence the "random" in Random Access Memory.

132. *See* Goldfoot, *supra* note 34, at 126–27 (noting RAM's temporary storage capability).

hands. Furthermore, investigators can extract some evidence that would not be found on long-term storage media from RAM, like passwords and encryption keys.[133]

Dynamic memory is advantageous because it is fast, but its downside is its volatility. Unlike magnetic or flash memory, a computer's RAM clears completely if the computer loses power or is turned off.[134] Because a computer's dynamic memory resets during a power loss, and because few forensics investigations occur immediately after a device's seizure, it is often difficult for investigators to recover evidence from RAM.[135]

Computers utilize both long- and short-term memory when performing tasks. Investigators can thus find evidence of crimes in both, so any lasting Fourth Amendment framework must consider the differences between the memory systems. However, understanding how digital storage operates is just one piece of a framework that must also account for the ways users and computers interact with the information in digital storage devices.

B. Digital Storage Applied: How Computers Use Memory

In addition to understanding where computers store information, judges applying Fourth Amendment precedent to digital memory devices must know how computers interact with that information. Judges without this background tend to base their analogies on their personal experiences with computers and may oversimplify or ignore the realities of digital storage.[136] Put simply, inaccurate understanding of computers leads to inaccurate analogies that, in turn, lead to bad legal precedent. To create a working Fourth Amendment framework for digital storage, one must understand the layers of interaction between users and their digital information.

---

133. *Id.*

134. BALAGURUSAMY, *supra* note 112, at 44.

135. Kedar Gupta & Alastair Nisbet, *Memory Forensic Data Recovery Utilising RAM Cooling Methods*, AUSTL. DIGIT. FORENSICS CONF. 11, 11 (2016).

136. *See generally* Stephanie A. Gore, *"A Rose By Any Other Name": Judicial Use Of Metaphors For New Technologies*, 2003 U. ILL. J.L. TECH. & POL'Y 403 (2003) (examining courts' use of metaphors to conceptualize new technologies); Douglas J. Gillan, Bruce S. Fogas, Suzanne Aberasturi & Shannon Richards, *Cognitive Ability and Computing Experience Influence Interpretation of Computer Metaphors*, 39 PROC. HUM. FACTORS ERGONOMICS SOC'Y 39TH ANN. MEETING 243 (1995) (describing people's tendency to use personal experiences when developing and interpreting technology-based metaphors).

Most computer users will never communicate with their computers in binary. Instead, users typically interact with their computers through a software interface called an Operating System ("OS").[137] The OS creates a platform for users to organize files in their storage and assign tasks to their computers.[138] The OS also manages all devices connected to a computer, interprets inputs, and generates the output display on a screen or monitor.

The central component of an OS is the File Explorer program, named "File Explorer" in Windows and "Finder" in MacOS.[139] In the File Explorer, users organize their files and programs into folders and subfolders.[140] Users also go to the File Explorer to access those files—that is, to task their computer to fetch the files from storage and display their contents.[141]

However, the OS's user interface merely translates what a computer does. It summarizes and reorganizes information to make it easier for users to understand. For example, when a user places a file into a new folder on the File Explorer, the computer does not move the physical location of the data in the storage to another physical location in the storage. Instead, the OS merely edits its registry so that the "new" file location in the Explorer is still pointing at the data stored in the "old" location.[142] The registry is a record that functions like a map the computer uses to know where files' clusters are physically located in the storage.[143] From the user's perspective, items in the same folder appear adjacent, but the items' data could be in different

137. Common consumer operating systems are Windows, Linux, and MacOS. *See* MORRISON ET AL., *supra* note 98, at 9–10.

138. *Operating System Summary*, ENCYC. BRITANNICA (2024), https://www.britannica.com/summary/operating-system [https://perma.cc/BU4H-A8UC].

139. *See generally* Houghton et al., *supra* note 120, at 79, 81 (calling file storage "instrumental").

140. *Working with the File Explorer in Windows 10*, GEO. UNIV. INFO. SERVS., https://uis.georgetown.edu/file-explorer [https://perma.cc/SA5L-99FC].

141. *Id.*

142. *See, e.g.*, B. Dawn Medlin, Joseph A. Cazier & Robert M. Weaver, *Consumer's PCs: A Study of Hard Drive Forensics, Data Recovery, and Exploitation*, 4 J. INFO. PRIV. & SEC. 3, 5–6 (2008) (describing this process for the special case when files are moved to the recycle folder).

143. *Id.*; *see also* C. Karamanolis, L. Liu, M. Mahalingam, D. Muntz & Z. Zhang, *An Architecture for Scalable and Manageable File Services*, HP LAB'YS., July 12, 2001, at 2–3 (describing how an object's "physical location" is decoupled from its "namespace" in a directory format).

physical locations. This discrepancy complicates applications of traditional Fourth Amendment doctrine, which often rely on objects' proximity to assess a search's reasonableness.[144]

Users generally do not interact directly with the computer's registry.[145] But, because the registry contains file metadata, including the records created when a user updates—that is, opens, edits, or saves—a file,[146] the registry is an important source of evidence. From it, investigators can recover information the user tried to hide by changing files' location or extension.[147] Investigators can also employ techniques like stochastic forensics[148] to the registry, allowing them to reconstruct the user's digital activity.[149]

Another difference between the common user experience and the realities of computer operation occurs when the user deletes a file. To the user, the file is gone, like a whiteboard wiped clean. But the OS does not physically purge that area in its memory. Instead, the OS edits the registry to indicate that the physical area is "unallocated" and can be overwritten when the user needs more space.[150] The information that made up the file continues to exist in the storage until it is overwritten by another file.[151] Investigators can access unallocated space and recover evidence of crimes that typical computer users do not even realize is still there.[152]

---

144. *See infra* Part III.B.1 (analyzing one such doctrine reliant on proximity).

145. *See* MORRISON ET AL., *supra* note 98, at 194 ("You should not change the registry."); Carol Silwa, *The Windows Registry*, COMPUTERWORLD (Apr. 29, 2002), https://www.computerworld.com/article/1328486/the-windows-registry.html [https://perma.cc/8DBC-98TP] (explaining that PC users do not know about or interact with the windows registry).

146. Ross Johnson, *Are You Mistakenly Destroying eDiscovery Metadata? Here's the Solution.*, GOLDFYNCH (Feb. 12, 2021), https://goldfynch.com/blog/2021/02/12/are-you-mistakenly-destroying-ediscovery-metadata-heres-the-solution.html [https://perma.cc/2B44-CRCR].

147. *See* Kerr, *Searches and Seizures*, *supra* note 43, at 544–45 (describing a forensic software with this capability); JOHN SAMMONS, THE BASICS OF DIGITAL FORENSICS 68–69 (1st ed. 2012) (listing several cases where investigators relied on registry evidence).

148. *See infra* note 265 and accompanying text (describing stochastic forensic techniques).

149. *Understanding Digital Forensics: Process, Techniques, and Tools*, BLUEVOYANT, https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools [https://perma.cc/3REB-993A].

150. *See* LEIGHTON R. JOHNSON III, COMPUTER INCIDENT RESPONSE AND FORENSICS TEAM MANAGEMENT: CONDUCTING A SUCCESSFUL INCIDENT RESPONSE 103–04, 126 (Mike Kessler ed., 2014) (describing the contents in and procedures of unallocated space).

151. Florian Weijers, Presentation and Evaluation of Common Methods of Deleting User Data in Common Computer File Systems (June 2022) (B.A. thesis, Hochschule Wismar) (ResearchGate).

152. *See generally* SAMMONS, *supra* note 147, at 65–80 (describing how to access the space).

Finally, the OS constantly updates and modifies files in a way that is indiscernible to users. Any time a user interacts with a file—moving its location, opening it, or making edits to it—the OS edits the file's metadata.[153] Investigators can use these metadata to compile information about a suspect's activity on the device.[154] However, investigators cannot access this information through the OS because, if the OS interacts with the files, it will remodify the metadata, essentially contaminating the evidence.[155]

An OS is a complex program. When users turn their computers on, the computers require an intermediary set of instructions to launch the OS and start up all the attached devices.[156] This intermediary program is called the basic input/output system ("BIOS"), and it handles the computer's boot process.[157] Users can access a BIOS interface by interrupting the computer's startup, which stops the normal boot sequence and prevents the OS launch.[158] After entering the BIOS, users can boot into a different software instead of the OS to access the computer's components.[159] Booting into a separate OS would benefit investigators because it would allow them to analyze aspects of the computer system without changing metadata, opening files, or displaying file contents on a monitor like they would if they booted into the OS.[160]

Courts have demonstrated a misunderstanding of the realities of digital storage and how users and computers interact with each other, leading to incomplete and inaccurate legal rules.[161] Having sufficient

153. *File Times*, MICROSOFT (Jan. 7, 2021), https://learn.microsoft.com/en-us/windows/win32/sysinfo/file-times [https://perma.cc/R6PZ-PPAB].

154. Dan Farmer, *What are MACtimes?*, DR.DOBB'S (Oct. 1, 2000), https://drdobbs.com/what-are-mactimes/184404275 [https://perma.cc/DL5Z-XLKN].

155. *Id.*

156. Ben Lutkevich, *BIOS (Basic Input/Output System)*, WHATIS.COM, https://www.techtarget.com/whatis/definition/BIOS-basic-input-output-system [https://perma.cc/9TQK-6ZXG].

157. *Id.*

158. *Id.*

159. *See* Barry Nauta, *Bootloaders — An Introduction*, 27–28 (Dec. 3, 2008), https://www.researchgate.net/profile/Barry-Nauta/publication/265323393_Bootloaders_-an_introduction/links/5a659ebb0f7e9b6b8fdc1bd7/Bootloaders-an-introduction.pdf [https://perma.cc/MJ6Z-99AX] (diagramming a computer's multiboot functionality).

160. Even though searching from the BIOS would be advantageous to investigators, I could not identify a jurisdiction that requires investigators to only search a computer from the BIOS.

161. *See infra* Part III.B (explaining how some such rules are inapplicable for digital storage).

background knowledge in these areas sets a foundation for a framework that better aligns with legal precedents and protects Fourth Amendment guarantees.

III. TRANSCRIPTION ERRORS: THE MISAPPLICATION OF PHYSICAL PRECEDENTS TO DIGITAL DEVICES

Against a proper framing of the physical components of digital storage devices and how users interact with them, courts' current approaches to applying the Fourth Amendment to digital storage are inadequate and ineffective. The legal system must adapt traditional search and seizure concepts to "modern, more sophisticated investigative tools."[162] Courts have tried to accomplish this goal through a variety of mechanisms, like adapting sixteenth-century doctrine to modern computers or inventing entirely new legal approaches. However, the Supreme Court has not provided a unified framework or consistent analytical method to evaluate the reasonableness of computer searches,[163] leaving lower courts to develop patchwork and sometimes self-contradictory doctrines.

Two areas of Fourth Amendment jurisprudence reveal the legal system's failure to account for the realities of digital storage. First, scholars' strained attempts to analogize drug-sniffing dogs to digital searches show why physical precedents cannot be used to protect digital privacy rights. Second, courts' patchwork application of the plain view exception demonstrates how courts' attempt to map old precedents onto modern problems harms individuals.

A. Don't Let the Dog Byte

Some courts and scholars analogize the forensic tools investigators use to search digital evidence to drug-sniffing dogs.[164] However, this flawed analogy demonstrates why physical precedents are not adequate to address the privacy concerns implicated by digital storage.

---

162. United States v. Ganias, 755 F.3d 125, 134 (2d Cir. 2014).

163. Smith, *supra* note 32, at 128.

164. *See generally, e.g.*, Burrows, *supra* note 38 (comparing digital searches to searches by drug-sniffing dogs); Tyler O'Connell, *Two Models of the Fourth Amendment and Hashing To Investigate Child Sexual Abuse Material*, 53 U. PAC. L. REV. 293, 317–19 (2021) (same); Goldfoot, *supra* note 34, at 141 (same); *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691 (2014) (same).

The Supreme Court has long upheld the constitutionality of using drug dogs without probable cause.[165] Because dogs do not "rummag[e]" through the contents of a sealed container and provide investigators limited information,[166] the use of dogs does not violate individuals' expectation of privacy. Yet a dog's signal generates sufficient probable cause to initiate a search without a warrant.[167] Dog sniffs are thus constitutional without a warrant and lead to constitutional warrantless searches, all while preventing excessive violations of privacy.[168]

Some scholars take these precedents and try to analogize digital storage forensic tools[169] to "digital dog sniffs."[170] For example, when comparing the use of digital forensics to drug dogs, scholars argue that certain software packages alert investigators only when something illegal is detected,[171] do not uncover the contents of closed files or applications,[172] and have a low false-positive rate.[173] However, these analogies justify an intrusion that is fundamentally unlike how drug dogs interact with individuals.

First, digital forensic tools process through every bit of information in a digital storage device. Although a dog can permissibly sniff around the *outside* of a vehicle without a warrant, it would undoubtedly violate the Fourth Amendment if a dog could enter *into* the vehicle and sniff around every nook before exiting to alert its

---

165. Irus Braverman, *Passing the Sniff Test: Police Dogs as Surveillance Technology*, 61 BUFF. L. REV. 81, 89–91 (2013).

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

167. Florida v. Harris, 568 U.S. 237, 246–48 (2013); Illinois v. Caballes, 543 U.S. 405, 409 (2005).

168. *See Data Mining, Dog Sniffs, and the Fourth Amendment*, *supra* note 164, at 705–06 (identifying the four conditions as "the sniff must only analyze information that is legally obtained; the sniff must only detect illegal activity; humans must not participate in any search until probable cause has been established by the sniff; and the sniff must have a low false-positive rate").

169. "Digital forensic tools" is a broad category of commercial software products that analyze digital storage devices like hashing. *See infra* notes 208–16.

170. *See Data Mining, Dog Sniffs, and the Fourth Amendment*, *supra* note 164, at 708 ("Given courts' fondness for reasoning by analogy in Fourth Amendment cases involving technological developments, it should be possible to design an automated search that replicates the core features identified in the dog-sniff cases . . . .").

171. Burrows, *supra* note 38, at 279.

172. O'Connell, *supra* note 164, at 319.

173. *Data Mining, Dog Sniffs, and the Fourth Amendment*, *supra* note 164, at 710.

handler.[174] Some argue that a software search does not violate people's expectations of privacy because it is not a "classic trespass," like physically entering someone's home, and thus "preserves the other 'privacies' contained within source files."[175] But the intrusiveness of digital searches—with respect to both their depth and their duration—destroys this analogy.[176] Permitting investigators to run software searches before obtaining a warrant is like permitting them to pull apart haystacks hoping to find a needle.[177]

Additionally, investigators have to reset the software's parameters for each search, a process that involves trying to predict what kind of evidence is stored on the device and adjusting settings to try to capture it.[178] Preparing and executing a digital forensic analysis thus "requires exercis[ing] . . . discretion that is not required when teaching a dog" to sniff for illegal substances.[179] Dogs do not have ulterior motives in their sniffs, but investigators can manipulate a forensic tool's parameters to circumvent constitutional safeguards.[180] Even though courts have tried to justify digital forensic tools by comparing them to drug dogs, the analogies' shortcomings reveal the legal system's failure to account for the realities of digital storage.

---

174. City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000).

175. O'Connell, *supra* note 164, at 319. By "other 'privacies,'" the author is likely referencing the contents of a digital storage device that are unrelated to the crime. The author describes forensic tools that analyze all the content in the digital storage but only alert investigators when they discover potential evidence. Although some say these search methods preserve the "privacies" of unrelated content, they still implicate Fourth Amendment concerns. *See infra* Part III.B.2.

176. *See* Burrows, *supra* note 38, at 280 ("[I]t is still possible that an investigator's hash analysis of a defendant's hard drive could appear more intrusive than a dog sniffing the outside of a bag."). Even if an individual intrusion does not implicate Fourth Amendment rights in and of itself, prolonged and extensive searches made possible by digitally archived evidence, in the aggregate, amount to a comprehensive examination of defendants. *See* Allyson Haynes Stuart, *A Right to Privacy for Modern Discovery*, 29 GEO. MASON L. REV. 675, 717–18 (2022) (calling this effect the "mosaic theory," where the comprehensive nature of digitally stored information increases the intrusiveness of a search of that information); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) (same).

177. *See* Goldfoot, *supra* note 34, at 140–41 (using a similar analogy).

178. *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 41 (2005) (noting that examiners adjust search criteria based on what they intend to find).

179. *Id.* at 46.

180. *See* Burrows, *supra* note 38, at 281 (implying investigators may run software improperly to satisfy "ulterior motives"); Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1205 (1995) (noting a potential for abuse).

B. Jurisdictional Split Screen: Applying the Fourth Amendment "Plain View" Exception

The inconsistent approaches to mapping the plain view exception to searches of digital storage is another microcosm of courts' and scholars' struggle to adapt physical precedents to the modern age. Under the plain view exception, investigators may search and seize items not described in a warrant if (1) they are not violating the Fourth Amendment to be in the location where they observe the items,[181] (2) they have a lawful right to access the object,[182] and (3) the items' incriminating nature is immediately obvious.[183]

It is well-established that suspects have a reasonable expectation of privacy in the contents of their digital storage devices implicated whenever an official begins a search of that storage.[184] However, courts and scholars have reached an impasse when determining how much data in a digital storage device fall within the authorization of a narrow warrant, what data are outside the scope of a warrant yet qualify for the plain view exception, and what evidence would still be impermissible to use in a criminal proceeding.[185] Unlike in the physical world, there are rarely tangible barriers separating information in digital storage,[186] and courts' analogies to physical precedent quickly break down.[187] Imperfect analogies threaten Fourth Amendment rights by muddying doctrine because they "ignore the realities" of modern

181. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).

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

183. *Id.* at 134–35 (1990); United States v. Montgomery, 527 F.3d 682, 687 (8th Cir. 2008).

184. Lindsay E. Harrell, Note, *Down to the Last JPEG: Addressing the Constitutionality of Suspicionless Border Searches of Computers and One Court's Pioneering Approach in* United States v. Arnold, 37 SW. U. L. REV. 205, 224 (2008).

185. Goldfoot, *supra* note 34, at 125 ("Regulating access to information . . . requires a decision: when does the forensic examiner access too much information? From the subcontainer perspective, this question becomes: what are the subcontainers? Or: where do we draw the barriers in the 'digital environment' to replace the missing physical barriers?").

186. *See supra* notes 57–62 and accompanying text (discussing digital data's intermingled nature); *supra* Part II.B. (discussing data storage location structure).

187. Goldfoot, *supra* note 34, at 113 ("Some physical rules cannot be applied to information at all, others might apply in multiple contradictory ways, and others, when applied, counter-intuitively produce results that barely restrict forensic examination at all.").

computing and result in the "oversimplif[ication] [of] complex area[s]" of law.[188]

Professor Orin S. Kerr, one of the leading scholars on the intersection of constitutional law and cybercrime, notes that there are three conflicting ways courts apply the plain view exception to digital storage.[189] Some courts view the entire contents of a storage device as a singular object, all of which may be searched as soon as one part is searched ("the single-thing approach"); other courts consider only viewed data as searched, "leav[ing] all unexposed information [as] unsearched"[190] ("the exposure approach"); and the remaining courts treat subdivisions within the storage—files, folders, or even components of files—as separate subcontainers to be searched individually ("the subcontainer approach").[191] The approaches are mutually exclusive, and the inconsistencies between them have led to a morass of new, competing rules[192] and patchwork applications[193] of the Fourth Amendment.

1. Viewing the Contents of a Storage Device as a Single Thing No Longer Computes. Some courts treat a digital storage device like a

188. O'Connell, *supra* note 164, at 320 (quoting United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999)); *see also* Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 122 (2008) ("Translating Fourth Amendment rules designed to regulate searches and seizures of physical property into rules that regulate digital investigations raises numerous questions.").

189. Kerr, *Searches and Seizures*, *supra* note 43, at 554.

190. *Id.*

191. Goldfoot, *supra* note 34, at 117 (explaining that parcels of information—like files or spreadsheet entries—"are each their own 'thing,' independent from each other and from the medium upon which they happen to be recorded" and the "medium, in turn, begins to look not just like an object, but like a virtual 'place' that contains those 'things'").

192. *Id.* at 113 ("Out of the resulting mess, many have called for departures from search and seizure law. . . . Far from permitting a straightforward application of old law to new facts, the subcontainer perspective leads to the invention of new rules, based on new policy choices.").

193. Roderick O'Dorisio, *"You've Got Mail!" Decoding the Bits and Bytes of Fourth Amendment Computer Searches After* Ackerman, 94 DENV. L. REV. 651, 663 (2017) ("In light of the sharp division among these federal circuit courts, the private search doctrine in computer searches is ripe for Supreme Court review.").

single piece of physical evidence.[194] Under the single-thing approach,[195] as soon as an investigator searches a portion of a device—even a single file—the owner loses all expectations of privacy for everything within the storage.[196] When courts use this approach, anything on the device is searchable under the plain view exception to the warrant requirement. The government could conceivably scrutinize millions of files and documents if it has authorization to access one file in the set.[197]

The Fourth Circuit adopted the single-thing approach in *United States v. Williams*.[198] In that case, the investigators' warrant authorized a search of various tangible devices and media located in the defendant's home.[199] But the court later held that the warrant "impliedly" extended to the contents of the defendant's digital storage, authorizing investigators to "open each file on [his] computer and view its contents."[200] Essentially, the court treated the contents of a storage device as inseparable from the device itself. A warrant authorizing the search and seizure of a device thus also authorized the search of everything stored on the device.

But the single-thing approach defies the Fourth Amendment's specificity requirement. Because digital storage contains so much intermingled and unrelated information,[201] authorization to search the

194. Smith, *supra* note 32, at 131 ("Ordinarily, district courts have held files on computers that were seized after having been used to commit crimes are forfeitable along with the physical computers themselves."); O'Dorisio, *supra* note 193, at 663 (noting that the Fifth and Seventh "circuit courts subscribe to the physical device framework, which holds that a search of a single file on a computer means the entire computer has been searched"). The Fourth Circuit also adopted this approach in *United States v. Williams*. *See infra* note 198 and accompanying text.

195. A related approach is to treat the physical device as a piece of evidence and all the digital data as separate "bins" of evidence. *See* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 88 (2005) ("[T]he warrant should state the physical evidence that the police plan to seize at the physical stage and the electronic evidence that the forensics analysts plan to search for at the electronic stage."). This Note treats these two approaches as the same because under either approach the court views the digital data as a homogenous whole.

196. O'Dorisio, *supra* note 193, at 663.

197. *Id.* at 675.

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

199. *See id.* at 515–16 (authorizing the search of physical "documents, photographs, and [i]nstrumentalities" and of devices, including "computer systems and digital storage media," but not explicitly authorizing the search of the content of those devices).

200. *Williams*, 592 F.3d at 521.

201. *See supra* note 30 and accompanying text.

entirety of a storage device is a modern general warrant.[202] This approach enables investigators to "access all the information stored on a hard drive regardless of whether that information has anything to do with the reason the computer is being searched,"[203] an intrusion that is out of line with the thrust of Fourth Amendment warrant protections.

2. Too Much Exposure for Exposure Approach. Some courts have rejected the single-thing approach and embraced the exposure approach to delineate when digital evidence has been searched within the meaning of the Fourth Amendment. This approach provides that only the information that appears on an output device and that investigators observe has been searched; all other information on the digital device is not searched and thus does not receive any legal protection.[204] In most cases, this limitation means investigators only search the files they click open, legibly display on a computer monitor, and see. Investigators can use digital forensic tools to manipulate and analyze all other data on the storage device without triggering Fourth Amendment scrutiny.

An advantage to the exposure approach, at least according to Kerr, is that it allows courts and investigators to ignore "technical details" and "behind the scenes" aspects of searching digital storage devices.[205] However, a deeper inquiry reveals that the exposure approach presents application problems and falls short of protecting individuals' expectation of privacy.

First, the exposure approach's vague standard presents tricky application problems for courts.[206] If the rule is that only observed data have been searched, courts must distinguish whether displayed data have been sufficiently "observed," a fact-intensive and ambiguous test. Factors like the amount of applied zoom, image pixelation, monitor

---

202. Delaware is one of several states to repudiate this approach. The state supreme court held that, "[g]iven the substantial risk that warrants for digital and electronic devices [may] take on the character of 'general warrants, [there must be] heightened vigilance . . . . [A] warrant must . . . be no broader than the probable cause on which it is based." Taylor v. State, 260 A.3d 602, 613–14 (Del. 2021) (internal quotations omitted); *see supra* notes 27, 87 and accompanying text.

203. Marc Palumbo, *How Safe Is Your Data?: Conceptualizing Hard Drives Under The Fourth Amendment*, 36 FORDHAM URB. L.J. 977, 978 (2009).

204. Kerr, *Searches and Seizures*, *supra* note 43, at 547.

205. *Id.* at 548.

206. O'Dorisio, *supra* note 193, at 675–76; *cf.* United States v. Ulbricht, 858 F.3d 71, 103 (2d Cir. 2017) ("[A]n invasion of a criminal defendant's privacy is inevitable, however, in almost any warranted search because in 'search[es] for papers, it is certain that some innocuous documents will be examined, at least cursorily, to determine whether they are, in fact, among those papers authorized to be seized.'").

screen brightness, or the investigator's attentiveness may obfuscate when cognizable observation occurs,[207] miring courts in difficult decisions with individuals' constitutional rights in the balance.

The exposure approach also justifies expansive searches using hashing techniques fundamentally at odds with Fourth Amendment protections. Hashing is a computer process that summarizes the information in a file into a string of thirty-two characters that uniquely identifies the file,[208] essentially the file's fingerprint.[209] Modern forensic tools permit investigators to hash every file on a digital storage device and automatically compare each file's hash number against a database of known hash numbers for previously seized illegal content.[210]

Under the exposure approach, even a complete storage hash does not constitute a search because no investigator has observed the files—only the forensic tool interacts with them.[211] First, the forensic tool flags any incriminating files. Then, the investigator requests a warrant based on the probability of finding evidence the investigator *already knows* is on the device.[212] Because hashing does not constitute a cognizable search, exposure approach jurisdictions permit warrantless hashing,[213] which is out of proportion with physical Fourth Amendment protections.

Imagine if officers could wait to obtain a warrant until after they enter and search a suspect's home and identify all potential evidence, requesting the warrant based on the knowledge they gained from the initial unauthorized search.[214] Just as this hypothetical undercuts the

207. O'Dorisio, *supra* note 193, at 676–77.

208. *What Is the MD5 Hashing Algorithm and How Does It Work?*, AVAST, https://www.avast.com/c-md5-hashing-algorithm [https://perma.cc/PQ2E-ED44].

209. *See, e.g.*, Burrows, *supra* note 38, at 262 (using the fingerprint analogy).

210. *Id.* at 261–64.

211. *See, e.g.*, United States v. Karo, 468 U.S. 705, 712 (1984) (holding the search to be constitutional because it "conveyed no information" to investigators); Kerr, *Searches and Seizures*, *supra* note 43, at 553 (citing to several Supreme Court opinions supporting this proposition).

212. Burrows, *supra* note 38, at 276–80.

213. Tiffany Ku, *State-Sponsored Hash Searches & the Reasonable Expectation of Privacy*, 69 HASTINGS L.J. ONLINE 28, 45–47 (2018).

214. This is distinct from the independent source doctrine, where evidence is inadmissible if obtained during an impermissible search. United States v. Bush, 727 F.3d 1308, 1316 (11th Cir. 2013).

plain view requirement of prior legal authorization,[215] so too hashing violates Fourth Amendment protections in a digital space. Additionally, hashing does not cease to be a search just because investigators are only presented with results and avoid seeing each individual file. Like the Supreme Court has held, "a search is a search, even if it happens to disclose nothing but the bottom of a turntable."[216] If the exposure approach justifies constitutional oversteps like hashing, it cannot be in line with the Fourth Amendment case law.

3. How Low Can You Go: Embracing the Subcontainer Approach. A competing application of the plain view exception to the warrant requirement divides a digital storage device into independent subcontainers, where opening each subcontainer constitutes a separate search.[217] Because individuals manifest a reasonable expectation of privacy in the information placed in a subdivision of storage—effectively closing that data in a subcontainer—accessing the information necessarily implicates a Fourth Amendment search.[218]

At least two federal circuits use the subcontainer approach.[219] These courts grant warrants authorizing investigators to access a specific portion of a digital storage device.[220] The warrant itself should define what the subcontainer is for that specific search—it could be a registry, folder, file, or something even smaller.[221] Courts can go as far as limiting each subcontainer to the contents of a single cell on a spreadsheet.[222] After securing the warrant, investigators can search everything in that subcontainer and seize any evidence related to the crime being investigated. They can also seize any evidence of other

215. *See supra* notes 181–203**Error! Bookmark not defined.** and accompanying text (explaining the requirements of plain view, including prior legal authorization).

216. Arizona v. Hicks, 480 U.S. 321, 325 (1987).

217. Goldfoot, *supra* note 34, at 118–19.

218. Harrell, *supra* note 184, at 223.

219. *E.g.*, United States v. Lichtenberger, 786 F.3d 478, 491 (6th Cir. 2015) (treating the contents of digital devices as subcontainers); *see also* Palumbo, *supra* note 203, at 978 (calling the subcontainer view the "minority approach").

220. *See, e.g.*, Palumbo, *supra* note 203, at 994–95 (using *Carey* to demonstrate the approach).

221. Goldfoot, *supra* note 34, at 112; *see also* Palumbo, *supra* note 203, at 979–80 (implying that, "[i]n practice," courts must determine "how broad or narrow the proper zone of search was drawn" to evaluate if "each file or folder" falls within the scope of the warrant).

222. *See* Goldfoot, *supra* note 34, at 119 ("Small portions of files, such as particular spreadsheet cells, can also be 'things,' and discrete things, at that.").

crimes discovered in that subcontainer under the plain view exception to the warrant requirement.[223]

However, the subcontainer approach can also generate difficult determinations for courts. Some warrants do not clearly define what that judge considers to be a subcontainer, forcing reviewing courts to "employ a special fact perspective" when evaluating the validity of a search after it has been performed.[224] Some courts even embrace this ambiguity by refusing to "address head-on" what the specific subcontainers were when reviewing a case,[225] leaving no guidance to determine when investigators exceed the authorization of their warrants.[226]

One bright-line rule some courts have drawn is to conceptualize each file on a digital storage device as a subcontainer.[227] Under this approach, investigators must have authorization to open a particular file. If they discover evidence by opening a file outside the scope of the warrant, that evidence will not be admissible in criminal proceedings.[228]

This test is easier for courts to apply. For example, in *United States v. Carey*, [229] the court decided that each file was an individual subcontainer. In that case, investigators had a warrant to search for evidence of drug trafficking.[230] During the course of his search, one investigator opened a JPEG file and discovered an image that appeared to contain child pornography.[231] The investigator proceeded

223. *See generally* James M. Rosenbaum, *In Defense of the Sugar Bowl*, 9 GREEN BAG 2d. 55 (2005), *reprinted in* 2006 FED. CTS. L. REV. 4 (discussing the plain view exception as applied to the subcontainer approach).

224. Goldfoot, *supra* note 34, at 112; Palumbo, *supra* note 203, at 979–80.

225. *See* Goldfoot, *supra* note 34, at 125 (noting that courts "seldom" identify the subcontainer).

226. *See* Wayne R. LaFave & Frank J. Remington, *Controlling the Police: The Judge's Role in Making and Reviewing Law Enforcement Decisions*, 63 MICH. L. REV. 987, 993 (1965) ("There is, for example, evidence that some judges issue search warrants without giving detailed consideration to whether sufficient grounds exist. Serious consideration of the legality of the search is postponed until the issue is raised by a motion to suppress.").

227. *See, e.g.*, United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (adopting, implicitly, the subcontainer approach by not extending the plain view exception past a single image file).

228. *Id.* at 1275–76. This Note refers to *Carey*'s application as the "file subcontainer approach."

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

230. *Id.* at 1270.

231. *Id.*

to open every JPEG on the defendant's computer until he stumbled across a cache of hundreds of images containing child pornography.[232]

The Tenth Circuit held that the investigator obtained the first image permissibly under the plain view exception[233] because its criminal nature was obvious and the investigator discovered the picture while conducting an authorized search.[234] However, the investigator had impermissibly expanded the scope of his search beyond the warrant's authorization by opening each subsequent JPEG file.[235] Because the files were "closed," they were "not in plain view," so the investigator collected all the remaining evidence of child pornography unconstitutionally.[236] The investigator could have used the first JPEG to obtain additional warrants to search the subsequent JPEGs, but his expanded search was not authorized based on the original warrant.

Treating individual files as subcontainers makes intuitive sense to casual computer users who deal with typical files.[237] On its face, the approach aligns with physical-world precedents.[238] But the subcontainer approach, alone, is insufficient to deal with the realities of digital storage. For example, how should courts treat a search of a drive's unallocated space? There are no distinct files there, but investigators can recover partial files and other data from these sections of digital storage devices. What about a drive's registries or a computer's RAM, areas that never store distinct files?[239] Should the whole space be a single subcontainer? The analogy breaks down even more when courts are faced with more advanced techniques, like stochastic forensics.[240] Investigators can recover meaningful evidence from all these locations, but none of them receive privacy protections from the plain view exception under the subcontainer approach.

---

232. *Id.* at 1271, 1273.

233. *Id.* at 1273.

234. *Id.*

235. *Id.*

236. *Id.*

237. A typical computer user will be familiar with the idea of opening, saving, and sorting individual files and documents. For many judges, this idea captures the nature of personal computers. *See, e.g.*, Goldfoot, *supra* note 34, at 126.

238. If one views a computer as a file management system, like a file cabinet, then the file subcontainer analogy is intuitive. Each file is "closed," and its relative proximity to other files does not matter because opening a file constitutes a new search. *See, e.g.*, *id.*

239. *See id.* at 126 ("RAM is not organized into files . . . . [and] forgets all data once the computer is turned off, a highly un-container-like habit. Moreover, RAM has no user-directed grouping . . . and is not rendered comprehensible by a user interface.").

240. *See infra* note 271 and accompanying text (discussing stochastic forensics in detail).

Furthermore, some judicial decision-makers are ill-suited to resolve these ambiguities ad hoc because the questions require an understanding of the technology that many judges lack.[241] For example, in *United States v. Crist*,[242] investigators were authorized to search part of a computer's magnetic hard drive.[243] The court stated that an examination of every part of the hard drive would constitute an impermissibly broad search.[244] But then the court erred while trying to decide what constituted the appropriate subcontainer, reasoning that because "a hard drive is comprised of many platters, . . . [e]ach platter, as opposed to the hard drive in its entirety, is analogous to a single [container.]"[245]

The *Crist* court misunderstood how hard drives work,[246] rendering its rule untenable.[247] However, *Crist*'s confusion is not inevitable. That court's problem came from its ad hoc determination of what constituted a subcontainer. *Carey*'s bright-line rule that a subcontainer is an individual file would have led to the correct outcome.

Unlike analogies to dog sniffs, the single-thing approach, and the exposure approach, *Carey*'s bright-line application of the subcontainer approach better conforms with Fourth Amendment requirements. Although the subcontainer approach, alone, would be an incomplete solution for investigators because it does not address the nonfile

241. *See* Dalia v. United States, 441 U.S. 238, 257 (1979) ("[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant . . . .").

242. United States v. Crist, 627 F. Supp. 2d 575 (M.D. Pa. 2008).

243. *Id.* at 582, 586.

244. *Id.* at 585–86 ("[T]he Government . . . applied the EnCase program to each compartment, disk, file, folder, and bit . . . . Such examination constitutes a search . . . . [T]he Court specifically rejects the Government's initial approach asking the Court to compare Crist's entire computer to a single closed container . . . ."). This was a rejection of the single-thing approach.

245. *Id.* at 586.

246. Burrows, *supra* note 38, at 275 ("Based on this strange analysis, it appears that the court does not understand the technology involved.").

247. *See supra* Part II (describing hard drive architecture). All the platters are attached to a single axle and spin at the same rate. A read/write head is paired to each platter and encodes a portion of a file onto its platter. For example, suppose a computer saves a document to a hard drive of n platters. Each platter would store $1/n$ of the document, and the hard drive could load that document n times faster than if the whole document was saved onto a single platter rotating at the same rate. Thus, the *Crist* rule is illogical because to load any file, the investigator would need to access all n platters.

information stored in the device, the subcontainer approach applied at an individual file level could serve as a component of a broader framework that translates Fourth Amendment protections to searches of digital storage.

IV. AN IMPERFECT SOLUTION

Considering the reality of digital storage architecture, the difficulty of mapping antiquated Fourth Amendment precedent onto digital storage, and the treatment that electronic devices already receive during searches and seizures, courts need a new scheme to conceptualize and enact investigative searches of digital storage devices. This Note proposes the following framework to resolve the ambiguities surrounding digital storage, return constitutionality inquiries to a reasonableness determination, and protect individual and state interests.

This Note's proposal embraces the file subcontainer approach and requires investigators to secure a pair of independent warrants before initiating a search of a digital device. In the first part of an investigation under the framework ("Phase One"), investigators receive a warrant authorizing the seizure of a digital storage device from the suspect. The investigators then use a forensic program to perform a limited examination of the storage. The program analyzes the subject's device and estimates the probability that the storage contains illicit material using techniques that fall short of a Fourth Amendment search per the file subcontainer approach.

Then, in the second part of the framework ("Phase Two"), the judge determines whether to authorize investigators to perform a Fourth Amendment search of the storage given the probability generated in Phase One and other relevant, case-specific factors.[248] Although this Note uses a hypothetical program to describe how the framework could work, the backdrop of Fourth Amendment case law defines the program's permissible limits.

This framework strikes a balance between the state's interest in collecting evidence of crimes and individuals' interest in protecting their information and, even more fundamentally, protection from unreasonable searches. No solution could guarantee collection of all

248. The other case-specific factors are those that are currently used in reasonableness weighing tests, like the state's interests, gravity of the alleged crime, and intrusiveness of the search, among others. *See, e.g.*, *supra* notes 68–70 and accompanying text.

evidence and full privacy protection because the only way to capture all evidence is to thoroughly search all devices. But, by providing judges with the probability that a device contains evidence of the crime before the judge authorizes a Fourth Amendment search, this framework would prevent investigators from searching some devices that do not contain evidence.

The repercussions of unjustified searches can be significant. Protection from unwarranted searches is among the most fundamental of rights.[249] Commentators have traced this protection to roots in natural rights, fundamental values, human dignity, and even economic motivations.[250] Violations of this right and can have "devastating effects."[251] Investigators can avoid violating individuals' rights without sacrificing the efficacy of their investigations by implementing the two-phase warrant framework outlined below.

A. Phase One: Initializing the Investigation.

To grant a search warrant, a judge must determine that the need to search the suspect's device outweighs the coextensive "invasion" of the suspect's privacy.[252] Except in the most extreme circumstances,[253] a judge should not grant a warrant unless an investigator can demonstrate a reasonable likelihood that evidence of a crime is contained on that device.[254] However, it may be impossible to know whether a given device contains evidence before examining it, which is why judges need an additional step—something to inform their determination of whether the likelihood that a device contains evidence is enough to justify the intrusion of a full-fledged search.

---

249. *See generally* Stuart, *supra* note 176 (treating the right to privacy as a fundamental right).

250. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 708 (1987).

251. Kerry & Morris, *supra* note 67.

252. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 536–37 (1967).

253. For a breakdown of some of the "exigent circumstances" that are considered exceptions to Fourth Amendment protections, see generally JAMES J. TOMKOVICZ & WELSH S. WHITE, CRIMINAL PROCEDURE: CONSTITUTIONAL CONSTRAINTS UPON INVESTIGATION AND PROOF 234–45 (Carolina Academic Press 7th ed. 2012).

254. *See* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) ("[P]robable cause is a reasonable ground for belief of guilt . . . . [This] mean[s] more than bare suspicion: Probable cause exists where the facts and circumstances . . . [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." (internal quotations omitted)).

Under this Note's framework, a criminal investigation begins without alteration. Investigators build a case indicating that a suspect may have evidence of a crime on digital storage devices. The investigators present their findings to a judge. If the judge agrees that the probability of finding incriminating evidence is sufficient, the judge grants a warrant authorizing the investigators to seize all the suspect's digital storage devices that might have the sought-after evidence.[255]

Because it is impossible to know on which device the suspect stores evidence of the accused crime, investigators run a program that performs a limited analysis of the device without going so far as to constitute a Fourth Amendment search per the file subcontainer approach in *Crist*.[256] For the sake of conciseness, call the program "ImperfectTool."[257] ImperfectTool analyzes the digital storage[258] and outputs a single number, ϕ, which is the probability a specific device contains the type of incriminating evidence investigators hope to collect. Investigators then use ϕ in Phase Two to obtain a second warrant authorizing a full search of the specific device(s) most likely to contain the sought-after evidence.

B. Phase Two: Executing the Fourth Amendment Search

After securing the suspect's digital storage devices and running ImperfectTool on them, the investigators have a ϕ for each device. The investigators then present the ϕs with their traditional evidence to the

255. For examples of the two-phase framework in use, see *infra* Part IV.B.

256. That is, the tool analyzes the storage without opening any individual file. *See supra* Part III.B.3.

257. Orin S. Kerr imagined a "Perfect Tool" that "sounds wonderful in theory" but "may not be possible." Kerr, *Searches and Seizures*, *supra* note 43, at 570. His "Perfect Tool" would "magically locate evidence described in a warrant." *Id*. Although the software in my proposal is not identical to Kerr's hypothetical program, the framework I propose would solve some of the problems Kerr identified in modern applications of Fourth Amendment doctrine. *See id.* (identifying efficiency, invasiveness, and overbreadth as problems); *infra* Part IV.C (explaining how ImperfectTool is a solution to these problems).

258. Commercially available forensics tools could perform the tasks required of the program in my proposal. For examples of toolkits that have capabilities similar to what I assign to ImperfectTool, see *Understanding Digital Forensics: Process, Techniques, and Tools*, BLUEVOYANT, https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools [https://perma.cc/JM3W-SZJB]; OpenText Security Cloud Team, *What's New in OpenText EnCase Forensic*, OPENTEXT BLOGS (Aug. 8, 2022), https://blogs.opentext.com/whats-new-in-opentext-encase-forensic [https://perma.cc/5YJ9-32BF]; Matt Zbrog, *A Guide to Digital Forensics and Cybersecurity Tools*, FORENSICS COLLS. (Mar. 24, 2024), https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools [https://perma.cc/P3K4-FXVL]. Although these toolkits can conduct the operations that ImperfectTool must perform, they violate Fourth Amendment precedent and do not operate in a two-phase warrant framework.

judge. The judge determines whether it is appropriate to perform a full search on each device.

This inquiry comports with any other warrant authorization—it is a reasonableness determination weighing the facts investigators presented against the intrusiveness of the search and the suspect's expectation of privacy. There is thus no bright-line threshold or rule—that is, if ϕ is greater than a certain value, the judge should grant a warrant. Rather, the judge must consider ϕ as a factor against the factual backdrop, including the gravity of the alleged crimes, risk of future criminal behavior, type of storage device and nonsuspect private information likely to be on the device, availability of other devices with higher ϕs, and other corroborating evidence. Judges already attempt to infer if devices likely have evidence.[259] Phase One merely provides a more solid foundation for their inference by producing a ϕ for each device.

If the judge determines that ϕ and the other factors do not establish sufficient probable cause to justify the intrusiveness of a thorough search, the judge should deny the Phase Two warrant application. Conversely, if the judge determines that ϕ and the other factors provide sufficient probable cause to justify a search of the digital storage device, the judge should grant the warrant. Depending on the factors, the judge may limit a search to specific subcontainers. However, given Phase One's additional safeguards, and because devices unlikely to contain evidence were removed for low ϕ values, in most cases the judge would likely authorize a thorough search of the whole device. The investigators can then proceed with a Fourth Amendment search, going file by file, hashing, or using any other forensic technique.

This outcome is preferable to the current system for several reasons. First, a device with a low ϕ likely contains private, noncriminal information in which the suspect has an expectation of privacy. The Fourth Amendment should shield this information from invasive searches, so the framework succeeds by preventing investigators from searching such devices.

Second, ImperfectTool's ϕ outputs would help investigators concentrate their efforts on the devices most likely to produce evidence

259. *See* Smith, *supra* note 32, at 130–31 (describing investigators' obligation to present evidence to judges making this determination under existing Fourth Amendment doctrine).

to advance their cases. Because people tend to have multiple digital storage devices, and because device capacity is increasing, exhaustively searching all of a suspect's digital storage in the hopes of finding something incriminating can be time and resource intensive. ImperfectTool's outputs allow investigators to skip devices unlikely to contain relevant evidence and focus their efforts on the storage devices with the highest probability of containing incriminating evidence. ImperfectTool thus benefits both suspects and investigators.

C. Reverse-Engineering a Black Box: Discerning ImperfectTool's Limits

Calling a hypothetical program "ImperfectTool" may seem abstract. However, the backdrop of case law prescribes ImperfectTool's limits, and modern forensic packages already have the capability to perform all of ImperfectTool's functions.[260]

The framework is based on the file subcontainer approach, by which a person maintains a reasonable expectation of privacy in individual files.[261] Under this framework, investigators cannot open files without violating the individual's privacy, even if only a program "sees" them. So ImperfectTool cannot open individual files. ImperfectTool also cannot hash because that necessarily involves individually processing files. However, under the file subcontainer approach, ImperfectTool can access all the information on the digital storage device that is not contained in files. This includes information saved in registries,[262] file metadata,[263] data in unallocated space,[264] and other stochastic information.[265]

Because investigators cannot open any file through the OS without violating the suspect's expectation of privacy[266] and altering

260. *See supra* note 258 and accompanying text (describing the capabilities of existing tools).

261. *See supra* notes 217–18 and accompanying text (highlighting the advantages of the subcontainer approach).

262. Information saved in registries might include file organization, density, and general storage information.

263. File metadata might include information about a filetype and when it was last accessed or altered.

264. Data in unallocated space might include incomplete remnants of deleted files.

265. Other stochastic information might include indications of patterns of usage, how much of the drive is encrypted, and other forensically significant data. *See generally*, *supra* Part 0I.B (describing how computers generate and store potentially relevant data); *see also infra* note 271 and accompanying text (describing stochastic forensic techniques).

266. *See supra* notes 217–18 and accompanying text (discussing the subcontainer approach).

associated evidence,[267] investigators must be able to run ImperfectTool without allowing the digital device to enter its OS. Thus, ImperfectTool must interrupt the device's startup sequence by booting from the BIOS.[268] This process is essential for two reasons. First, booting from the BIOS prevents the device's OS from booting, so ImperfectTool can perform its analysis without altering the storage, preserving evidence's integrity.[269] Second, if investigators boot to the OS before running ImperfectTool, data on the storage would necessarily be exposed to investigators, meaning investigators would perform a Fourth Amendment search without a warrant. For example, the investigators might see the lock screen, profile image, items on a desktop or home screen, or usernames. All these exposures are unconstitutional intrusions of privacy.[270] Booting to ImperfectTool from the BIOS prevents even these minor intrusions.

By analyzing the nonfile features in a digital storage device, ImperfectTool could estimate the probability that the device contains illegal information. For example, ImperfectTool could look for directories with gigabytes of files hidden in unallocated space, frequently accessed files, "red flag" words in filenames and extensions, illegal or suspicious programs, and patterns indicating illegal use to determine the likelihood that the device contains evidence of a crime.[271] After analyzing these data and case-specific inputs from investigators, ImperfectTool produces an output ϕ showing the probability that the device contains evidence of a particular crime.[272]

---

267. *See supra* notes 153–55 and accompanying text (highlighting file metadata).

268. *See supra* notes 156–60 and accompanying text (describing BIOS booting).

269. *See supra* notes 153–54 and accompanying text (explaining that OS booting modifies files).

270. *See generally supra* Part 0III.B.2 (arguing that unwarranted exposure itself is impermissible).

271. Stochastic forensics is one of several forensic techniques that extract evidence from digital devices. The technique involves analyzing patterns of nonartifact computer elements to infer device usage. *See, e.g.*, Goldfoot, *supra* note 34, at 127 ("Just as forensic pathologists can examine a cadaver's fractures, bruises, calluses, and scars to determine what happened to that body over a person's lifetime, so too can a computer forensic analyst examine a hard drive to learn how a computer was used."). For an explanation of how these elements could be used as evidence of nefarious activity, see generally Jonathan Grier, *Detecting Data Theft Using Stochastic Forensics*, 8 DIGITAL INVESTIGATION S71 (2011).

272. ImperfectTool will thus work like the program suggested by the author of *Data Mining, Dog Sniffs, and the Fourth Amendment*, *supra* note 164. That author described a program that

Of course, this means that ImperfectTool will never be 100 percent reliable. The program could occasionally give false negatives, or low ϕs, for devices that contain evidence. As a result, a judge may not authorize a Phase Two warrant, and these evidence-riddled devices could evade investigation. Conversely, ImperfectTool may give false positives, or high ϕs, for devices that do not contain evidence. This could lead a judge to authorize a Phase Two warrant, permitting an invasive search on a device containing no evidence of a crime. However, the two-phase framework, on net, would still be better than the current warrant process.

The only way to know for sure that a device has evidence of a crime is to conduct a thorough search until evidence is found. Similarly, the only way to know for sure that a device contains no evidence of a crime is also to complete a thorough search. But this method is unreasonably invasive.[273] The ImperfectTool two-phase warrant framework strikes a balance between the state's interest in collecting evidence and the suspect's privacy interests. Certainty cedes some ground to preserve privacy, which aligns with all other Fourth Amendment reasonableness tests. ImperfectTool is *necessarily* imperfect because it is a compromise between these interests. Although some evidence of criminal activity likely will remain undetected,[274] this framework hedges against the oversearch of many devices justified under the current system.[275]

Incorporating ImperfectTool into the two-phase warrant framework would also resolve the ambiguity surrounding courts' current applications of Fourth Amendment precedents to digital spaces.[276] This approach would both protect individuals' privacy

---

could analyze databases of legally obtained information and suggest potential criminals. *See id.* at 709 ("To simplify . . . the algorithm might render a result of 'p(terrorist) = 0.9.'"). However, that program has several undesirable attributes. First, that program relies on an existing database of contraband. *Id.* Second, investigators use that program to skim data of individuals who are not suspected of a crime, leading to "concerns over impermissibly biased analysis." *Id.* at 709 (calling this a "concern . . . until there has been a highly reliable indication of probable cause for illegal activity"). Finally, that program's probability could only be used to obtain a first warrant, whereas ImperfectTool's probability would justify an exhaustive search of data already seized by investigators. ImperfectTool thus "offers the potential to . . . satisfy[] a number of both constitutional and privacy concerns" that the author of *Data Mining* did not consider. *Id.* at 712.

273. *See supra* note 26 and accompanying text (discussing a similar prolonged, exhaustive search).

274. *Cf. infra* Part IV.D.

275. *See supra* notes 26–27 and accompanying text (discussing an example of a search of multiple devices that did not contain any illegal material).

276. *See infra* Part IV.D.

interests in their digital information and help investigators conduct more efficient searches of devices.

Finally, the framework remains workable as more users transition their data storage from personal devices to remote servers. Fourth Amendment protections continue to apply even when an individual places their information online.[277] Because servers store information the same way as personal long-term memory devices,[278] courts could apply the two-phase warrant framework the same way to data on the cloud as they would to a personal computer. This framework thus would remain a workable approach to protect individuals' fundamental Fourth Amendment right to be "secure in their persons . . . and effects, against unreasonable searches and seizures"[279] for the foreseeable future.

D. The Last Bit: Applying the Two-Phase Framework

This Note's framework can protect suspects' rights yet still lead to the successful prosecution of criminals. For example, the investigators in *United States v. Mann* had probable cause that Mann stored evidence of voyeurism on a digital storage device.[280] But investigators did not know *which* devices contained the evidence.[281] Investigators searched through each storage device, one at a time, over months before figuring out which one contained the locker room images.[282] But, if that court had followed the two-phase warrant approach, Mann's privacy rights would have been protected, investigators would have efficiently found evidence of both voyeurism and child pornography, and Mann still would have faced justice.

The investigators easily could have secured the first warrant in Phase One. The judge authorized investigators to thoroughly search

277. Wessler, *supra* note 32 ("[O]ur sensitive information does not lose Fourth Amendment protections merely because we store that information on a 'third party' server . . . .").

278. *See* Michael Jones, *Anatomy of a Cloud Storage Infrastructure*, IBM DEV. (Nov. 30, 2010), https://developer.ibm.com/articles/cl-cloudstorage [https://perma.cc/R2BC-7L3G] (noting that cloud servers "implement[] the physical storage for data"); *What is a Data Center?*, AMAZON data centers as "physical locations" for storing "computing machines" and "related hardware").

279. U.S. CONST. amend. IV.

280. United States v. Mann, 592 F.3d 779, 780–81 (7th Cir. 2010).

281. *See id.* (noting that the investigators searched all devices, including those without evidence).

282. *Id.* at 781.

his other digital storage and would likely have authorized the substantially less intrusive Phase One search under this Note's framework. The investigators would then have used ImperfectTool to analyze Mann's digital storage devices. The device where he actually stored the voyeuristic videos likely would have returned a high ϕ value because it contained hundreds of pictures and video files with file names and content that would have set off red flags for ImperfectTool.[283] The investigators would likely have received the Phase Two warrant to search just that storage device because of its high ϕ value.

While searching that storage device, investigators would have encountered both evidence of voyeurism and child pornography images. All that evidence falls within the plain view exception to the warrant requirement as implemented in this Note's framework. The investigators could bring child pornography charges against Mann and use the images they discovered to establish probable cause to search his other digital devices with high ϕs for more illegal images.

Mann has a better outcome under this Note's framework than the actual case for three reasons. First, the two-stage warrant requirement preserves the privacy of Mann's noncriminal information on the devices that contained no evidence. Even though Mann is an unsympathetic defendant, the process and precedent matter—an oversearch is a constitutional violation regardless of whether it produces evidence.[284] Second, the investigators concentrate their effort on the devices with incriminating evidence instead of wasting it on the devices without evidence. And third, Mann faces the same charges and therefore is held accountable for his crimes.

Similarly, *Carey* would have had a better outcome under this framework.[285] In that case, the Tenth Circuit ruled that the investigator had abandoned his initial search for evidence of drug trafficking after he saw a pornographic image and began opening other JPEG files.[286] Under the framework, the investigators would have conducted Phase One, and ImperfectTool would have alerted them to a high probability of illicit content on the device. Consequently, a judge would have

283. *See id.* (finding evidence that Mann had visited the site "Perverts Are Us" in the computer's files among other indicia of child pornography consumption).

284. *See supra* notes 249–51 and accompanying text (describing the negative consequences of unnecessary privacy violations and the democratic ideals underlying Fourth Amendment rights).

285. *See supra* notes 229–36 and accompanying text (discussing *Carey*'s outcome).

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

authorized investigators to conduct a comprehensive search. All the evidence the investigators encountered would arise out of a constitutional search because the "subsequent photos" would be within the scope of the Phase Two warrant. Because the two-phase framework narrows the scope of the search to a specific device likely to have illicit content, and because suspects do not have a reasonable expectation of privacy to illicit content, investigators in that case would not have been penalized for stumbling across evidence of a separate crime.

Finally, the two-phase warrant framework prevents misapplications of Fourth Amendment precedent like the failed platters rule in *Crist*.[287] Judges do not need to stretch analogies from physical space to fit digital storage—the framework already accounts for the realities of digital storage. This Note's framework merely provides judges an additional datapoint to consider when determining if a search of a digital device is reasonable.

CONCLUSION

Courts should implement this novel framework to moderate the seizure and search of private digital storage devices. No tool could truly be perfect—some evidence of criminal activity cannot be found without exhaustively searching every device. But the two-phase warrant framework described above would conform better with physical precedents, allow investigators to operate more efficiently, and apply justice consistently without significantly decreasing the efficacy of forensic investigations.

287. United States v. Crist, 627 F. Supp. 2d 575 (M.D. Pa. 2008); *see supra* notes 242–47 and accompanying text (explaining the *Crist* Court's error).