NEW YORK LAW SCHOOL

NYLS Law Review

Volume 67
Issue 1 *Spotlight on Student Scholarship: Part I*

Article 3

January 2023

Securing the "Privacies of Life" by Preventing General Searches of Computers

Patrick Fischer

VOLUME 67 | 2022/23

PATRICK FISCHER

Securing the "Privacies of Life" by Preventing General Searches of Computers

67 N.Y.L. Sch. L. Rev. 29 (2022–2023)

EDITOR'S NOTE: Patrick Fischer was a Staff Editor of the 2021–2022 *New York Law School Law Review*. He received his J.D. from New York Law School in 2022.

I. INTRODUCTION

The Fourth Amendment "secure[s] 'the privacies of life' against 'arbitrary power'"[1] and protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[2] Specifically, the Fourth Amendment establishes the warrant requirement mandating that police officers obtain a warrant supported by probable cause and particularity before commencing a search.[3] The Fourth Amendment prevents general exploratory searches, which threaten privacy rights by giving police officers unfettered discretion to comb through a person's effects, because the particularity requirement directs police officers seeking a warrant to specify the place to be searched and evidence to be seized.[4]

An exception to the warrant requirement is the plain view doctrine, which allows police officers to collect evidence not specifically enumerated in a warrant, so long as they find the evidence in plain view in an area they are lawfully permitted to search and the criminal nature of the evidence is "immediately apparent."[5] The Supreme Court has emphasized that the plain view doctrine does not run afoul of the Fourth Amendment's prohibition on general searches, because the particularity requirement still limits the areas and items police officers may search.[6]

But issues arise regarding how to apply the Fourth Amendment to computers, which store enormous amounts of sensitive personal and third-party information.[7] The search of a computer tends to yield more information than even the search of a home,[8] and so the particularity requirement is of great importance when police officers search a computer.[9] Yet limiting the scope of computer searches has proved challenging for courts, because it is difficult for police officers to know where particular files are located on a computer or what they contain, especially since files can be mislabeled,

1. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

2. U.S. Const. amend. IV.

3. *See id.*

4. *See id.*

5. Horton v. California, 496 U.S. 128, 133–37 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) (plurality opinion)).

6. *Id.* at 139.

7. "Sixteen gigabytes" of data alone "translates to millions of pages of text, thousands of pictures, or hundreds of videos." Riley v. California, 573 U.S. 373, 394 (2014). And today, personal computers typically provide 250 gigabytes of storage. Armin Tadayon, *Preservation Requests and the Fourth Amendment*, 44 Seattle U. L. Rev. 105, 127 (2020).

8. *See Riley*, 573 U.S. at 396–97.

9. United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009); *see also* United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 579 F.3d 989, 1004 (9th Cir. 2009) (en banc) ("Th[e] pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." (citation omitted)), *revised per curiam by* 621 F.3d 1162 (9th Cir. 2010).

encrypted, or concealed.[10] Instead, courts frequently authorize police officers to search an entire computer to ensure they can find the relevant evidence sought in their warrant.[11]

However, in the 2009 case *United States v. Comprehensive Drug Testing, Inc.* (*CDT II*), the U.S. Court of Appeals for the Ninth Circuit adopted five prophylactic rules to address the issues that computer searches pose to the particularity requirement.[12] The *CDT II* rules were meant to protect individuals' privacy interests by limiting the scope of computer searches conducted by law enforcement.[13] Nevertheless, because of the burdens they imposed on the government's ability to investigate crimes, the rules were criticized by other courts[14] and subsequently abandoned by the Ninth Circuit.[15]

Courts remain split on the issue of how to limit warrants for computer searches. Some courts allow police officers to search every file on a computer without any restrictions.[16] Other courts require that police officers search only the files reasonably necessary to find the evidence sought in their warrant, a restriction that effectively grants police officers broad discretion to rummage through all files given the challenges officers face in pinpointing responsive data.[17]

This Note contends that a modified set of the *CDT II* prophylactic rules is needed to balance individuals' privacy rights with the government's interests in investigating crimes. A reintroduction of the *CDT II* rules is validated by a series of recent Supreme Court cases that offer stronger protections against the threat to privacy posed by

10. *See, e.g.*, United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010); *see also CDT II*, 579 F.3d at 1004 ("There is no way to be sure exactly what an electronic file contains without somehow examining its contents . . . .").

11. Meghan Holloway, Comment, *Penalty Default Rules for Digital Searches: Why Courts Should Spur Legislative Action via Second-Order Regulation*, 87 U. Chi. L. Rev. 1395, 1403 (2020); *see, e.g.*, United States v. Cobb, 970 F.3d 319, 332–33 (4th Cir. 2020).

12. 579 F.3d at 1006. A discussion of the rules articulated in *CDT II* can be found in Section IV, *infra* pp. 40–42.

13. *See CDT II*, 579 F.3d at 1006.

14. James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809, 2844 (2011); *see also* United States v. Mann, 592 F.3d 779, 785–86 (7th Cir. 2010); United States v. Stabile, 633 F.3d 219, 241 n.16 (3d Cir. 2011).

15. United States v. Comprehensive Drug Testing, Inc. (*CDT III*), 621 F.3d 1162 (9th Cir. 2010) (per curiam), *revising* 579 F.3d 989 (9th Cir. 2009) (en banc). For a discussion of the effect of *CDT III* on Ninth Circuit law, see *infra* note 97.

16. *See, e.g.*, *Cobb*, 970 F.3d at 332 (noting that "a computer search must . . . authorize at least a cursory review of each file on the computer" (quoting United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010))).

17. *See, e.g.*, United States v. Loera, 923 F.3d 907, 917–20 (10th Cir. 2019) (stating that a digital search should be "reasonably directed at uncovering the evidence specified in the search warrant" but acknowledging that some searches will require an "item-by-item review" of files).

computer searches.[18] Moreover, this Note proposes novel modifications to the *CDT II* rules to alleviate some of the burdens they imposed on the government.

Part II of this Note discusses the origins of the Fourth Amendment and the development of the plain view doctrine. Part III highlights recent Supreme Court jurisprudence protecting Fourth Amendment privacy rights against the realities of digital searches. Part IV discusses the particularity requirement and the plain view doctrine: the challenges of their application by courts, and the inadequacies of existing solutions, including search protocols and the *CDT II* rules. Part V argues that the Court's recent decisions addressing digital searches justify reviving the *CDT II* rules, but that modifications to these rules are necessary to protect the government's interest in investigating crimes. Part VI concludes this Note.

II. THE HISTORY OF THE FOURTH AMENDMENT AND THE DEVELOPMENT OF THE PLAIN VIEW DOCTRINE

During Britain's colonial rule of America in the 1760s, courts issued writs of assistance that served as general warrants permitting British officers to search any home for contraband.[19] These writs gave British officers unbridled discretion to dig through the belongings in colonists' homes and were therefore "reviled" by the colonists.[20] Massachusetts colonist James Otis challenged the validity of these writs under English common law in 1761.[21] Otis lost the case, but John Adams saw in this fight the beginning of the colonists' quest for independence.[22] After the Revolutionary

18. United States v. Jones, 565 U.S. 400, 404–05 (2012); Riley v. California, 573 U.S. 373, 401–03 (2014); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

19. *Writ of Assistance*, Black's Law Dictionary (11th ed. 2019).

20. *Riley*, 573 U.S. at 403. The controversy over the writs in Britain and colonial America was the origin of the famous maxim that "a person's home is their castle" and should not be easily intruded into by the government. Barry Friedman & Orin Kerr, *Common Interpretation*, *The Fourth Amendment*, Nat'l Const. Ctr., https://constitutioncenter.org/the-constitution/amendments/amendment-iv/interpretations/121 (last visited Feb. 11, 2023).

21. *James Otis*, Encyc. Britannica, https://www.britannica.com/biography/James-Otis (last visited Feb. 11, 2023). Otis found the writs to be "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book." Boyd v. United States, 116 U.S. 616, 625 (1886) (quoting Thomas M. Cooley, A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union 301–03 (Boston, Little, Brown, & Co. 1868)).

22. Friedman & Kerr, *supra* note 20. Adams described the effect of Otis's courtroom argument against the writs:

> Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance. Then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.

Letter from John Adams to William Tudor (Mar. 29, 1817), *in* 10 The Works of John Adams 247–48 (Charles Francis Adams ed., Boston, Little, Brown, & Co. 1856).

War, the Founders in 1791 wrote the Fourth Amendment into the Constitution to safeguard against writs of assistance and general warrants.[23]

Today, under the Fourth Amendment, a search performed without a warrant is "presumptively unreasonable."[24] To obtain a warrant, police officers must specify the items they intend to seize, the particular place they intend to search, and the probable cause to believe that evidence will be found in that particular location.[25] Further, general exploratory searches are prohibited.[26] To prevent general searches, courts must issue warrants with particularity.[27]

The Supreme Court has carved out several exceptions to the warrant requirement, including the plain view doctrine.[28] This doctrine allows police officers to seize an item not specified in a warrant if the officers discover the item in plain view in an area they lawfully access and the criminal nature of the item is "immediately apparent."[29] For example, if police officers have a warrant for a stolen television, they may not use the plain view doctrine to seize evidence inside a closed drawer.[30] The drawer falls outside the scope authorized by the search warrant, because such a large item could not reasonably be stored in a drawer.[31]

The 1971 Supreme Court plurality opinion *Coolidge v. New Hampshire* articulated the plain view doctrine and explained that the particularity requirement ensures that the doctrine "does not convert [a] search into a general or exploratory one" prohibited by the Fourth Amendment.[32] The plain view doctrine as expressed by the plurality in *Coolidge* permitted police officers to seize evidence not specified in a warrant when the officers had a warrant or some other legal ground to search an area for specific

---

23. *See Riley*, 573 U.S. at 403. The Fourth Amendment provides

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

24. Horton v. California, 496 U.S. 128, 133 (1990).

25. *See* U.S. Const. amend. IV.

26. *See* Andresen v. Maryland, 427 U.S. 463, 480 (1976) ("[T]he problem [posed by the general warrant] is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings." (alterations in original) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (plurality opinion))).

27. *Id.*

28. *Horton*, 496 U.S. at 133.

29. *Id.* at 136–37 (quoting *Coolidge*, 403 U.S. at 466 (plurality opinion)). The Court has reasoned that "[i]f an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy." *Id.* at 133.

30. People v. Hughes, 958 N.W.2d 98, 116 (Mich. 2020).

31. *See id.*

32. *Coolidge*, 403 U.S. at 465–67 (plurality opinion).

items and, during that search, inadvertently found another item that was criminal in nature in plain view.[33]

The Supreme Court modified the plain view doctrine in the 1990 case *Horton v. California* by discarding the requirement that evidence in plain view be found inadvertently.[34] The Court reasoned that eliminating this requirement would better achieve "evenhanded" policing and, further, would not turn a valid warrant into a general warrant because the particularity requirement would still restrict the scope of the search.[35] Thus, per *Horton*, the modern three-part test to seize evidence under the plain view doctrine requires that police officers are lawfully present in the area where the item is found, the officers have lawful access to the item, and the incriminating nature of the item is "immediately apparent."[36]

III. THE SUPREME COURT, THE FOURTH AMENDMENT, AND DIGITAL SEARCHES

An individual has a strong privacy interest in the data on their computer.[37] Computers store personal information like photographs, text messages, internet browsing history, and location records that collectively allow the government to piece together a person's private interests, associations, and movements.[38] In several recent cases, the Supreme Court has adapted traditional Fourth Amendment principles to protect these "privacies of life"[39] against intrusive digital searches by the government.[40]

Generally, a "search" occurs, for the purposes of the Fourth Amendment, when the government physically intrudes onto an individual's person or property[41] or infringes on an individual's reasonable expectation of privacy.[42] The Supreme Court has consistently held that police officers tracking a car traveling in public does not

33. *Id.* at 464–71. For instance, if, while executing a search warrant for a stolen television perched on a console with a wide-open drawer, police officers happen to notice that the open drawer is filled with illegal drugs, the officers could seize the drugs under the plain view doctrine. *See Hughes*, 958 N.W.2d at 116.

34. 496 U.S. at 130.

35. *See id.* at 138–40.

36. *Id.* at 136–37 (quoting *Coolidge*, 403 U.S. at 466 (plurality opinion)).

37. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (finding that a person has a privacy interest in the collection of their movements through Global Positioning System tracking); Riley v. California, 573 U.S. 373, 403 (2014) (determining that a person has a privacy interest in their cell phone data); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (concluding that a person has a reasonable expectation of privacy in their cell-site location information).

38. *Riley*, 573 U.S. at 394–95; *see also* United States v. Ganias, 824 F.3d 199, 218 (2d Cir. 2016) (noting that a digital storage device can hold data "roughly equal to 16 billion thick books" (quoting Quentin Hardy, *As a Data Deluge Grows, Companies Rethink Storage*, N.Y. Times, Mar. 15, 2016, at B3)).

39. *Riley*, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

40. *See id.* at 401–03; *Jones*, 565 U.S. at 404–05; *Carpenter*, 138 S. Ct. at 2216–17.

41. Olmstead v. United States, 277 U.S. 438, 465–66 (1928).

42. Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).

constitute a "search" because a driver has no expectation of privacy in their whereabouts in public.[43]

However, in its 2012 decision *United States v. Jones*, the Supreme Court held that the government conducted a Fourth Amendment "search" by attaching a Global Positioning System (GPS) tracking device to the undercarriage of the defendant's vehicle and tracking it for twenty-eight days.[44] Though the majority relied on the traditional trespass doctrine to resolve the case,[45] five justices appeared ready to adopt a new Fourth Amendment theory that "depart[ed] dramatically from existing doctrine."[46] Specifically, Justice Samuel Alito's concurring opinion, joined by three other justices[47] and endorsed by Justice Sonia Sotomayor in her separate concurrence, articulated the mosaic theory later embraced by the Court.[48] Under the mosaic theory, the government conducts a Fourth Amendment "search," and therefore must obtain a warrant, if its actions over time would amount to a "collective 'mosaic' of surveillance," even if no one individualized action would constitute a "search" on its own.[49]

Additionally, the search incident to arrest doctrine is a traditional exception to the warrant requirement that permits police officers to seize and inspect items they find on an arrestee after an arrest occurs.[50] The Court has routinely applied this "well[-]settled" and "broadly stated" exception.[51]

43. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that the defendant driving his car on public roads "ha[d] no reasonable expectation of privacy in his movements from one place to another" because he "conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property"); United States v. Karo, 468 U.S. 705, 721 (1984) (concluding that beeper surveillance revealing a truck's route on public streets was not a search).

44. 565 U.S. at 403–05.

45. *Id.* at 404–05 (determining that a "search" occurred when the government physically intruded onto the defendant's private property to attach the GPS tracker).

46. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 346 (2012).

47. Justice Alito's concurring opinion was joined by Justices Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan. *Jones*, 565 U.S. at 418–31 (Alito, J., concurring in the judgment).

48. *Id.* at 430 (noting that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period"); *id.* at 416 (Sotomayor, J., concurring) (suggesting that "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on" is material to determining whether a "search" occurred); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.").

49. Kerr, *supra* note 46, at 313. Under the mosaic theory, a "search" is defined "as a collective sequence of steps rather than as individual steps." *Id.* For example, a one-time surveillance of a church, a bar, a gym, or a home may bare very little private information about an individual, but frequent surveillance of those locations can expose whether an individual "is a weekly church goer, a heavy drinker, a regular at the gym, [or] an unfaithful husband." United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 565 U.S. 400 (2012).

50. United States v. Robinson, 414 U.S. 218, 224 (1973).

51. *Id.* at 224–26.

Nevertheless, in its 2014 decision *Riley v. California*, the Court held that police officers without a warrant were not permitted to rely on the search incident to arrest doctrine to inspect cell phones.[52] The Court refused to expand the search incident to arrest doctrine to cell phones because it found cell phone data to be uniquely personal and "qualitatively different" than the physical objects previously considered under the doctrine.[53]

The third-party doctrine is another traditional exception to the Fourth Amendment's warrant requirement, which allows the government to access the personal information an individual voluntarily shares with a third party, such as telephone numbers or bank records.[54] The Supreme Court has consistently applied this doctrine on the ground that an individual assumes the risk that the information they disclose to a third party could, in turn, be shared with others.[55]

Yet, in its 2018 decision *Carpenter v. United States*, the Court held that the government could not use the thirty-party doctrine to access the defendant's cell-site location information (CSLI)[56] without a warrant.[57] The Court emphasized that CSLI, unlike telephone numbers and bank records, collects people's movements, which can expose intimate information about their lives.[58]

Jones, *Riley*, and *Carpenter* afford stronger Fourth Amendment protections against digital searches and reflect the Court's growing concern about the threats that new technologies pose to privacy rights. The lower federal courts, however, have struggled to adapt the traditional Fourth Amendment principles of particularity and the plain view doctrine to protect privacy rights in computer searches.[59]

IV. PROBLEMS WITH APPLYING THE PARTICULARITY REQUIREMENT AND THE PLAIN VIEW DOCTRINE TO COMPUTER SEARCHES

The Fourth Amendment prohibits general exploratory searches of a person's belongings.[60] To prevent these types of searches from occurring, courts are required to issue warrants with particularity.[61] This is meant to ensure that "nothing is left to

52. 573 U.S. 373, 386 (2014).

53. *Id.* at 393–97. Instead, the Court offered a "simple" solution to police officers: They can obtain a warrant to search a defendant's cell phone. *Id.* at 403.

54. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

55. *See id.*

56. CSLI is time-stamped data created by cell phone providers that shows which cell towers a cell phone contacted when a particular communication was made. *See id.* at 2211.

57. *Id.* at 2217, 2223.

58. *Id.* at 2217–18.

59. *See* United States v. Perez, 712 F. App'x 136, 139 (3d Cir. 2017) (noting that courts have failed to effectively "adapt Fourth Amendment search doctrines designed for physical spaces to digital contexts").

60. Andresen v. Maryland, 427 U.S. 463, 480 (1976).

61. Marron v. United States, 275 U.S. 192, 196 (1927).

the discretion of the officer executing the warrant."[62] But because broad searches are often necessary to find relevant information on computers, courts have failed to tailor the particularity requirement to the digital context. The result is that police officers search through more information than would be permitted in the physical world, and the information gleaned may be seized under the plain view doctrine.[63] This, of course, threatens basic Fourth Amendment privacy rights.[64]

The majority of circuits attempt to limit the scope of computer searches and, as a result, the digital evidence susceptible to the plain view doctrine.[65] Specifically, these courts require police officers conducting a digital search to follow two requirements that minimize the nonresponsive data they encounter. First, police officers must reasonably direct their search toward finding the evidence sought in their warrant.[66] Second, police officers are only permitted to look at a digital file for the time it

62. *Id.*; *see also* United States v. Chadwick, 433 U.S. 1, 9 (1977) ("The judicial warrant has a significant role to play in that it provides the detached scrutiny of a neutral magistrate, which is a more reliable safeguard against improper searches than the hurried judgment of a law enforcement officer 'engaged in the often competitive enterprise of ferreting out crime.'" (quoting Johnson v. United States, 333 U.S. 10, 14 (1948))).

63. *See* United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1117 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part) (observing that automatically allowing the government to search an entire computer based on a warrant to search for some information on that computer amounts to "a breathtaking expansion of the 'plain view' doctrine").

64. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (warning that the government's power to collect private data using technology, if not limited, could "alter the relationship between citizen and government in a way that is inimical to democratic society" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring))).

65. *See* United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013) (noting that a warrant to search electronic records "(1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized"); United States v. Galpin, 720 F.3d 436, 441, 448 (2d Cir. 2013) (holding that a search warrant was unconstitutionally overbroad when it allowed police officers to search "[a]ny [c]omputers, central processing units, external and internal drives, storage units or media terminals[,] and video display units" for evidence); United States v. Triplett, 684 F.3d 500, 506 (5th Cir. 2012) (concluding that, during computer searches, police "officers should limit [their] exposure to innocent files" only); United States v. Rarick, 636 F. App'x 911, 916 (6th Cir. 2016) (determining that a search was reasonable when the police officer "targeted his search to where he reasonably believed the [evidence] was most likely to be found"); United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010) (instructing police "officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described"); United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008) (rejecting the argument that a lack of search protocols in a warrant for a computer search invalidated the warrant but recognizing that search protocols may be necessary at times); United States v. Johnston, 789 F.3d 934, 942 (9th Cir. 2015) (reviewing a policer officer's search of a computer to ensure the methods he employed did not amount to "digging around" or otherwise occasion the need for another warrant); United States v. Loera, 923 F.3d 907, 920 (10th Cir. 2019) (counseling police officers to "[n]arrowly tailor[] search methods" toward finding evidence responsive to their warrant); *In re* Search of Apple iPhone, 31 F. Supp. 3d 159, 169 (D.D.C. 2014) ("Until the government actually explains how the search will proceed, and thus how the government intends to limit its search of data outside the scope of the warrant, th[e] warrant cannot be issued.").

66. *See Galpin*, 720 F.3d at 451–52; *Rarick*, 636 F. App'x at 916; *Mann*, 592 F.3d at 786; *Johnston*, 789 F.3d at 941; *Loera*, 923 F.3d at 917.

reasonably takes to determine whether the file is responsive to their warrant.[67] These protections, though, are illusory, because courts following this approach recognize that searches of entire computers are often necessary and continue to grant police officers broad discretion to rummage through significant amounts of private data.[68]

The minority approach, followed by the U.S. Courts of Appeals for the Third, Fourth, and Eleventh Circuits, gives police officers the discretion to conduct at least a cursory scan of every electronic file during a digital search.[69] These courts reason that evidence can be hidden anywhere on a computer.[70] This approach explicitly authorizes general searches; it abandons the particularity requirement entirely and provides no real restrictions on the government's search of a computer.[71]

The U.S. Court of Appeals for the Tenth Circuit has slightly modified the approach followed by the majority of courts to limit the scope of digital searches and still considers whether police officers found evidence inadvertently when determining if evidence was properly seized under the plain view doctrine.[72] Though the Tenth Circuit recognizes that inadvertence is no longer required for a proper plain view seizure of physical evidence under Supreme Court precedent, it "include[s] inadvertence as a factor" when applying the plain view doctrine to digital searches, which are less

---

The reasonableness of the search method will depend on the case. *See Loera*, 923 F.3d at 917–19. Courts instruct police officers to narrowly tailor a digital search by first searching in the "most obvious" locations and, if unsuccessful, only then gradually expanding to more "obscure" areas. *Id.* at 920 (quoting United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009)). However, courts do not require that particular search method in all cases; for instance, when a computer's files are disorganized, courts recognize that police officers may have to search most, if not all, of its files. *Id.*; *see, e.g.*, *Johnston*, 789 F.3d at 942–43 (holding that a digital search was reasonable when the police officer performed a "'bare minimum' forensic scan of the computer" and then used a search tool to find responsive evidence).

67. *See Loera*, 923 F.3d at 917–19 (explaining that a one-minute search of nonresponsive files is reasonable, but a five-hour search of nonresponsive data is unreasonable); United States v. Ulbricht, 858 F.3d 71, 101–02 (2d Cir. 2017) (holding that a cursory search of nonresponsive files was reasonable).

68. *See Burgess*, 576 F.3d at 1094 (stating that, in certain cases, "there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders"). For example, one court explained that police officers searching for evidence of drug crimes have little reason to search through a folder labeled "2002 Tax Return" but then conceded that the officers could still search the folder for drug-related files. *Id.* at 1094 & n.19.

69. United States v. Vetri, 811 F. App'x 79, 82 (3d Cir. 2020) (holding that a warrant authorizing review of all electronic files during a digital search was not overbroad); United States v. Cobb, 970 F.3d 319, 332–33 (4th Cir. 2020) (finding that a preliminary search of every file on a computer was constitutional); United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009) (holding that a police officer had a "lawful right" to search every electronic file on a defendant's hard drives to find responsive evidence).

70. *See, e.g.*, *Vetri*, 811 F. App'x at 82; United States v. Williams, 592 F.3d 511, 521–22 (4th Cir. 2010).

71. *See* People v. Hughes, 958 N.W.2d 98, 117–18 (Mich. 2020) (determining that allowing police officers to search an entire cell phone based on the chance that evidence could be found anywhere on it "would effectively nullify the particularity requirement . . . and rehabilitate an impermissible *general warrant*," which "would be especially problematic in light of *Riley*'s" concerns about the amount of data stored on a cell phone).

72. *Loera*, 923 F.3d at 919–20. No other circuit has explicitly considered inadvertence as a factor in determining whether digital evidence was properly seized under the plain view doctrine. *See, e.g.*, *Williams*, 592 F.3d at 523 (rejecting the inadvertence requirement for digital searches based on Supreme Court precedent).

likely to be restricted by warrants.[73] However, the Tenth Circuit's requirement that police officers find evidence inadvertently is not an effective limitation because, like the majority of courts, the Tenth Circuit continues to validate broad digital searches[74] and the Supreme Court has consistently disfavored inquiring into the subjective mindsets of police officers when considering Fourth Amendment violations.[75]

Additionally, search protocols are ex ante limitations imposed by courts on how police officers conduct digital searches.[76] For example, a court can mandate search protocols that require police officers executing a computer search to use only particular forensic tools, search only certain file types,[77] or perform specific keyword searches.[78] Accordingly, search protocols can be manipulated to constrain the scope of a computer search and the nonresponsive files police officers encounter.[79] Of course, these ex ante protocols also hinder law enforcement's ability to discover relevant evidence, because digital evidence may be mislabeled, encrypted, concealed, or otherwise difficult to find.[80] In practice, then, police officers must often violate search protocols and rummage to find relevant data.[81]

Because of the practical burdens that search protocols impose on the government, courts have generally been reluctant to mandate these limitations.[82] Further, courts traditionally seek to avoid interfering with how law enforcement executes warrants.[83]

73. *Loera*, 923 F.3d at 919 n.3 (citing Horton v. California, 496 U.S. 128, 130 (1990)).

74. *See* United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009).

75. *See, e.g.*, *Horton*, 496 U.S. at 138 (reasoning that, with respect to the plain view doctrine, an objective standard rather than a subjective standard would better serve "evenhanded" policing). Additionally, proving a police officer's subjective mindset is difficult. Craig M. Bradley, *The Reasonable Policeman: Police Intent in Criminal Procedure*, 76 Miss. L.J. 339, 343 (2006) (noting that a police officer's subjective mindset is "difficult to ascertain and easy to fabricate").

76. Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1242 (2010).

77. Adam M. Gershowitz, *The Post-*Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585, 633 (2016).

78. Stephen Guzzi, Note, *Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search-Protocol Warrant Restrictions*, 49 Am. Crim. L. Rev. 301, 319 (2012).

79. *See id.*

80. *See* Comput. Crime and Intell. Prop. Section Crim. Div., U.S. Dep't of Just., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 79 (2009) (warning that requiring search protocols has "the potential to seriously impair the government's ability to uncover electronic evidence" because police officers under restrictions "will fail to find many kinds of files that fall within the scope of [the] warrant"); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 575 (2005) (finding that "[i]t is generally impossible to know" the search techniques police officers will need to use before a computer search begins).

81. *See* Saylor, *supra* note 14, at 2856.

82. United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011); *see also* United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) (finding that limiting the scope of a computer search through search protocols is "unrealistic").

83. *See* Dalia v. United States, 441 U.S. 238, 257 (1979) (observing that "it 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").

In addition, valid concerns exist about whether judges, most without computer forensics expertise, can and should set search protocols.[84] Ultimately, because search protocols impede investigations and are not routinely mandated by courts, they are not a viable standalone solution to limit searches of computers.

In *CDT II*, the Ninth Circuit acknowledged the government's interest in finding responsive evidence during computer searches, but cautioned that broad authorization threatens to turn every warrant to search a computer into a general warrant.[85] The court attempted to reconcile these competing concerns by fashioning five requirements the government must satisfy to obtain a warrant for a digital search.[86]

Under the *CDT II* rules, first, the government must waive reliance on the plain view doctrine, neutralizing the risk that the doctrine would turn a broad digital search into a general search.[87] Second, the government is required to enlist specialized government computer personnel or an independent third party to segregate seizable from non-seizable data.[88] Under this requirement, police officers involved in an investigation could not examine or retain files that they do not have probable cause to search.[89] Third, in its warrant application, the government must disclose the risks of evidence being destroyed and the prior efforts exerted to obtain the same or related evidence.[90] This third requirement is consistent with the government's "duty of candor in presenting a warrant application."[91] Fourth, the court must preapprove search protocols tailored to find only the data for which there is probable cause.[92] Court-ordered search protocols ensure that an investigation remains focused on finding the relevant evidence.[93] Lastly, the government must destroy or return to the owner nonresponsive data and inform the court of the data it has retained, destroyed,

84. *See* Kerr, *supra* note 80, at 575 (explaining that "judges are poorly equipped to evaluate whether a particular search protocol" will be needed because most judges "have only a vague sense of the technical details of how computers work").

85. 579 F.3d 989, 1004 (9th Cir. 2009) (en banc), *revised per curiam by* 621 F.3d 1162 (9th Cir. 2010). At issue in *CDT II* was a government investigation into the Bay Area Lab Cooperative's alleged involvement in distributing illegal steroids to Major League Baseball players. *Id.* at 993. The government had obtained a warrant to seize, amongst other evidence, electronic files from Comprehensive Drug Testing, Inc., a third-party company that had administered drug tests to the baseball players. *Id.*

86. *Id.* at 1006.

87. *Id.* at 997–98, 1006.

88. *Id.* at 999–1000, 1006 ("If the segregation is to be done by government computer personnel, [the government] must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.").

89. *See id.*

90. *Id.* at 998, 1003–04, 1006.

91. *Id.* at 998–99, 1004 ("More than one of the judges involved in this case below commented that they felt misled or manipulated by the government's apparent strategy of moving from district to district and judicial officer to judicial officer in pursuit of the same information, and without fully disclosing its efforts elsewhere.").

92. *Id.* at 999–1000, 1006.

93. *See id.* at 999–1000.

or returned.[94] The rationale underpinning this final requirement is that the government should not benefit from information it seizes unlawfully.[95]

When the government petitioned for a rehearing en banc,[96] the Ninth Circuit refused to rehear the case and instead issued a 2010 per curiam opinion, *United States v. Comprehensive Drug Testing, Inc.* (*CDT III*), abandoning the *CDT II* rules altogether.[97] The court in *CDT III* acknowledged, however, that "the daunting realities of electronic searches" demand "greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."[98]

The *CDT II* rules are flawed. First, they burden the government.[99] In particular, the rules requiring the government to waive the plain view doctrine and access only seizable data unduly restrict the scope of a search.[100] Moreover, *CDT II*'s search protocol requirement is impractical because it prevents the government from finding evidence responsive to its warrant[101] and raises concerns about whether judges lacking

94. *Id.* at 1000–01, 1006.

95. *Id.* at 1003.

96. After the Ninth Circuit's decision in *CDT II*, then-solicitor general Elena Kagan petitioned for a rehearing en banc, arguing that the court erred in concluding that the government must waive the plain view doctrine. *See* Brief for the United States in Support of Rehearing En Banc by the Full Court at 14–15, *CDT III*, 621 F.3d 1162 (9th Cir. 2010) (per curiam) (Nos. 05-10067, 05-15006, 05-55354) [hereinafter Brief for the United States]. She argued that evidence found under the plain view doctrine is "the fruit of constitutionally permissible activity" and that requiring the government to waive the doctrine could lead to loss of evidence. *Id.* at 14. Specifically, the brief discussed a case in which the government found child pornography in plain view when executing a warrant to search a computer for environmental crimes and emphasized that the evidence could not have been used if the government had been required to waive reliance on the plain view doctrine under *CDT II*. *Id.* at 15.

97. 621 F.3d 1162.

In his concurring opinion in *CDT III*, Chief Judge Alex Kozinski advocated that the *CDT II* rules should remain as "guidance" to magistrate judges in issuing warrants for digital searches. *Id.* at 1179–80 (Kozinski, C.J., concurring). Nevertheless, "[t]he concurrence [wa]s not joined by a majority of the en banc panel and accordingly the suggested guidelines are not Ninth Circuit law." *Id.* at 1183 (Callahan, J., concurring). After *CDT III*, the Ninth Circuit has emphasized that the *CDT II* rules are only advisory and has followed the approach taken by the majority of courts to limit the scope of digital searches. United States v. Schesso, 730 F.3d 1040, 1049 (9th Cir. 2013) (noting that there are "no clear-cut rule[s]" for computer searches).

98. *CDT III*, 621 F.3d at 1177.

99. *See* Brief for the United States, *supra* note 96, at 14.

100. *See id.* (arguing that waiving the plain view doctrine under *CDT II* "could result in the loss of highly probative evidence about the very crime under investigation, such as when a warrant contains a date restriction but the resulting search turns up evidence that the crime began or continued after officers previously had reason to believe"); Bryan K. Weir, Comment, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 Geo. Mason U. C.R.L.J. 83, 103 (2010) (pointing out that, under *CDT II*, the government can never use any files outside the scope of its warrant, as it would be able to do in a physical search).

101. *See* Brief for the United States, *supra* note 96, at 15–16 (contending that the *CDT II* search protocol requirement is "[u]nworkable" because search protocols are "grossly inefficient, lead to delays in obtaining time-sensitive evidence, and heighten the risk that important information will be missed").

technical backgrounds can and should order search protocols.[102] Lastly, other circuit courts have rejected the *CDT II* rules as overbroad, especially absent Supreme Court precedent authorizing the abandonment of the plain view doctrine in the context of digital searches.[103]

The Court determined that the plain view doctrine would not lead to general searches because the particularity requirement would still restrict the scope of a search.[104] However, in the digital world, courts continue to grant police officers broad authorization to search computers, and, thus, warrants for digital searches are issued without sufficient particularity. This broad authorization risks turning computer searches into general searches because police officers access greater quantities of information and more opportunities to seize information they discover in plain view.[105] Moreover, the existing solutions to limit the scope of computer searches—specifically search protocols and the *CDT II* rules—are neither workable nor consistently applied. Consequently, the plain view doctrine threatens the "privacies of life"[106] that digital devices contain and, like the traditional Fourth Amendment doctrines in *Jones*, *Riley*, and *Carpenter*, must be reworked.

V. PROPOSED SOLUTION: A MODIFIED SET OF THE *CDT II* RULES

Particularity and the plain view doctrine must be reconsidered in light of the dangers that technological innovations pose to individuals' privacy rights under the Fourth Amendment. Though flawed, the *CDT II* rules provide a strong foundation for addressing these dangers. However, the rules must be altered to better balance investigative and privacy interests.[107] Thus, courts should apply the following modified set of the Ninth Circuit's prophylactic rules to limit the scope of computer searches.[108]

First, similar to the rule in *CDT II*, the search of a computer should be performed by an independent digital forensic analyst who reasonably targets their search toward

---

102. *See* Kerr, *supra* note 80, at 575.

103. *See, e.g.*, United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010); United States v. Stabile, 633 F.3d 219, 241 n.16 (3d Cir. 2011).

104. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (plurality opinion); Horton v. California, 496 U.S. 128, 139–40 (1990).

105. *See CDT II*, 579 F.3d 989, 998 (9th Cir. 2009) (en banc) ("If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file—and we have no cavil with this general proposition—then everything the government chooses to seize will, under this theory, automatically come into plain view."), *revised per curiam by* 621 F.3d 1162 (9th Cir. 2010).

106. Riley v. California, 573 U.S. 373, 403 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

107. *See CDT II*, 579 F.3d at 1006 ("Everyone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment.").

108. This Note focuses only on *CDT II* rules regarding the execution of, and not the application for, a warrant, and so omits discussion of the need to disclose the risks of destruction of data in a warrant application. *See id.* at 1006.

uncovering, and providing the government with, responsive data only.[109] This segregation requirement protects privacy interests because it effectively satisfies the particularity requirement and minimizes the nonresponsive data seen by any party.[110] Importantly, this rule does not burden the investigation, as the independent digital forensic analyst ensures that the government receives all evidence for which it has probable cause to search.

Second, as mandated in *CDT II,* the government should be required to waive the plain view doctrine. Although the first rule is effective in reducing the amount of data the government gains access to and consequently may seize under the plain view doctrine,[111] the doctrine still poses a threat to privacy because, following segregation, even responsive files could include evidence of multiple crimes.[112] Requiring the government to waive the plain view doctrine with this second rule protects Fourth Amendment privacy interests during a digital search by assuring that particularity is met and eliminating any incentive a third party might have to conduct an exploratory search.[113] Moreover, the alternative, redacting the nonresponsive data from responsive files turned over to the government, would thwart the government's efforts to interpret the responsive data.[114]

Third, unlike in *CDT II*, the government should not be required to follow court-ordered search protocols. Eliminating this rule alleviates a massive burden on the

109. The independent digital forensic analyst should use expertise, tools, and techniques to target their search toward finding responsive data. *See* United States v. Loera, 923 F.3d 907, 918 (10th Cir. 2019). Further, the analyst should start their search in the area where responsive data is most likely to be found, gradually expanding their search to less obvious areas only if necessary. *See id.* at 920. Lastly, the analyst should be permitted to search an entire computer only if they first report that files are concealed or manipulated. *See* People v. Hughes, 958 N.W.2d 98, 121 (Mich. 2020).

110. *See* Weir, *supra* note 100, at 103. Even if a broad warrant is granted to search the contents of a computer, the particularity requirement is satisfied because the government is only provided with information that is responsive to its warrant.

111. *See id.* at 113 ("The abolition of the plain view doctrine, which the Ninth Circuit's proposed solution *effectively accomplished with its first two criteria*, guarantees the type of protection the Fourth Amendment requires." (emphasis added)).

112. *See* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomms. & Tech. L. Rev. 39, 105 (2002). Two scholars described this threat as follows:

> [A] [responsive] file may not only contain information about the crimes currently being investigated, the file may also contain information about other criminal activity. Since the officers have been given lawful access to the entire file, the plain view doctrine comes into play and lets the officers observe, and seize, information falling into the second category.

Id.

113. *See CDT II*, 579 F.3d at 998 (finding that waiver of the plain view doctrine for digital searches is necessary to prevent the government from "tak[ing] everything back to the lab, hav[ing] a good look around and see[ing] what [it] might stumble upon"); Weir, *supra* note 100, at 113 (arguing that, if the plain view doctrine is abandoned, "[a]n unscrupulous government agent no longer has an incentive to broaden [their] search beyond the particularity of the warrant because a broader search cannot bear any fruit").

114. *See* Brenner & Frederiksen, *supra* note 112, at 105 ("[R]edacting portions of a file could result in the officers' receiving fragmentary and essentially useless evidence, which would hamper, if not obstruct, the officers['] investigation.").

government by removing the practical barriers search protocols raise for police officers.[115] Further, forgoing this rule does not compromise privacy interests because the other modified rules are a sufficient safeguard.

Finally, to the extent the independent digital forensic analyst returns nonresponsive data to the government inadvertently, the government should be required to destroy or return the nonresponsive information to its owner, like in *CDT II*. This requirement respects the owner's privacy interest and places no additional burden on the government, which is not entitled to use nonresponsive information after waiving the plain view doctrine.

At least two arguments against this Note's proposed solution are anticipated. The first criticism these proposed rules will likely face is that they unduly burden the government and hinder its ability to investigate crimes.[116] But this is not so. The Supreme Court has consistently held that the focal point of the Fourth Amendment analysis is reasonableness.[117] And the modified *CDT II* rules proposed in this Note are reasonable, because they balance the government's investigative interests with individuals' strong privacy interests in their data during computer searches.

Though police officers will no longer be able to use evidence found in plain view that is outside the scope of their warrant, officers will still obtain evidence for which they have probable cause to search since the independent digital forensic analyst will deliver responsive files and search protocols will not frustrate the investigation. Any financial and investigative burdens the government may endure under the modified rules are outweighed by the need to prevent unconstitutional digital searches. Additionally, although *Jones*, *Riley*, and *Carpenter* did not directly address particularity, these cases demonstrate that it would be unreasonable not to enhance the particularity requirement in computer searches, because stronger protections are needed to shield the "privacies of life"[118] in the digital era.

Second, critics will question whether the ex ante procedures in this modified approach are constitutional.[119] Although courts have traditionally been hesitant to adopt ex ante rules, the Supreme Court has never explicitly found them unconstitutional in the context of digital searches.[120] Furthermore, *Jones*, *Riley*, and *Carpenter* have

115. *CDT II*'s search protocol rule is effectively replaced by the first rule this Note proposes requiring an independent digital forensic analyst to reasonably direct their search toward finding responsive data, which achieves the same ends but places less of a burden on the government.

116. *See, e.g.*, *CDT II*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part) (expressing concerns about the financial costs of using specialized government computer personnel or independent third parties to perform computer searches); Weir, *supra* note 100, at 115 (noting that the *CDT II* rules may require the government to establish a new department for computer searches); Brief for the United States, *supra* note 96, at 14 (arguing that *CDT II*'s requirements will cause evidence to be lost).

117. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (observing that reasonableness is "the ultimate touchstone of the Fourth Amendment").

118. *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

119. *See, e.g.*, Kerr, *supra* note 76, at 1246 ("[E]x ante regulation of computer warrants is both constitutionally unauthorized and unwise.").

120. *See* Gershowitz, *supra* note 77, at 622.

demonstrated that traditional rules must be revisited in light of technological changes in order to preserve the privacy rights the Fourth Amendment was intended to protect. The case for modifying the traditional particularity requirement and the plain view doctrine during digital searches should be no different.

VI. CONCLUSION

Individual privacy rights form the bedrock of our nation's principles, and the Founders developed the Fourth Amendment particularity requirement to protect the people against searches that disregarded these rights. Today, however, the particularity requirement provides little actual protection against broad computer searches because it is difficult for police officers and courts to predict where on a computer evidence is stored. Although courts have consistently recognized the privacy interests compromised in digital searches, they have done almost nothing to restrict the government's ability to search digital data. Moreover, the Supreme Court highlighted the problems inherent in digital searches in *Jones*, *Riley*, and *Carpenter* and warned against giving the government unbridled power when technology is involved.

The *CDT II* rules were created to combat the constitutional privacy issues that arise in computer searches but, in practice, were too burdensome on the government. The modified *CDT II* rules proposed in this Note would better balance the government's interests with the people's.