Fordham Urban Law Journal

Volume 46
Number 1 *Contemporary Urban Issues*

Article 4

2019

Bits, Bytes, and Constitutional Rights: Navigating Digital Data and the Fourth Amendment

Stephen Moccia

BITS, BYTES, AND CONSTITUTIONAL RIGHTS: NAVIGATING DIGITAL DATA AND THE FOURTH AMENDMENT

Stephen Moccia[*]

INTRODUCTION

The invention of computers, like all modern technologies, was revolutionizing.[1] Modern storage mechanisms can contain the equivalent of sixteen billion thick books.[2] One 2017 study found that eighty-nine percent of consumers check their smartphones within an hour of waking up and, on average, look at their phones approximately forty-seven times each day (a statistic that rises to eighty-six times a day for eighteen to twenty-four year olds).[3] *Forbes* reports that, by 2020, about 1.7 megabytes of new information will be created every second for every person, with total accumulated digital data growing to around forty-four zettabytes, or forty-four trillion gigabytes.[4] By that same year, the "Internet of Things"[5] will have

---

* J.D., 2018, Fordham University School of Law; B.A., 2012, Fordham College at Rose Hill. The author would like to thank Professor Deborah W. Denno, Arthur A. McGivney Professor of Law, for her support and encouragement during the production of this Note, his former cybercrime colleagues for both their training and their continued guidance in preparing this Note for publication, and his friends and family for providing thoughtful advice, edits, and assistance throughout this process.

1. *See, e.g.*, Sherry Turkle, *How Computers Change the Way We Think*, CHRON. HIGHER EDUC. (Jan. 30, 2004), https://www.chronicle.com/article/How-Computers-Change-the-Way/10192 [https://perma.cc/5K4K-9KQ2].

2. *See* Quentin Hardy, *As a Data Deluge Grows, Companies Rethink Storage*, N.Y. TIMES (Mar. 14, 2016), https://www.nytimes.com/2016/03/15/technology/as-a-data-deluge-grows-companies-rethink-storage.html [https://perma.cc/D8RA-6FWU].

3. *See* DELOITTE, GLOBAL MOBILE CONSUMER SURVEY: US EDITION, THE DAWN OF THE NEXT ERA IN MOBILE 2 (2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf [https://perma.cc/CX8D-PX24].

4. *See* Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, FORBES (Sept. 30, 2015, 2:19 AM), https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read [https://perma.cc/4DL6-RBMU]. To offer a sense of scale, removable thumb drives available at retail stores typically range from about two gigabytes to sixty-four gigabytes. Manufacturers estimate that a two-gigabyte flash drive can store approximately 110 average-sized image files, five minutes of high-definition video, and 125 MP3 files; a sixty-four-gigabyte flash drive can hold 2000 average-sized image files, 160 minutes of high-definition video, and 4000 MP3 files. *See, e.g.*, *Number of Photos, Songs, Documents, and Video Hours a SanDisk Cruzer USB Flash Drive Can Hold*, SANDISK, https://kb.sandisk.com/app/answers/detail/a_id/462/~/number-of-photos%2C-songs%2C-documents%2C-and-video-hours-a-sandisk-cruzer-usb-flash [https://perma.cc/PAE9-YNPR].

5. The "Internet of Things" is shorthand for the proliferation of ordinary objects that are interconnected through the Internet, enabling them to send or receive data and operate "intelligently" without human interaction. Examples range from a smart thermostat or home appliance that can be controlled remotely and that may know the optimal settings and schedule to minimize the homeowner's energy consumption, to wearable devices that collect and aggregate a person's health data. The Internet of

grown to over fifty billion connected devices worldwide.[6] Thus, digital storage devices are, more and more, the spaces in which people operate — replacing the hard-copy physical world of the past. Yet, the innovators behind such creations are aware of basic human nature and have historically employed a style of design in which digital elements resemble real-world objects that anyone would recognize.[7] What is now common was not always so familiar,[8] so technology developers relied heavily upon real-world analogs — such as "files," "documents," a "desktop," "trash bins," "tabs," "folders," and "cutting and pasting" — to make computers more intuitive.[9] The standard interface of a computer—what is called the Graphical User

---

Things can also have commercial applications, with industrial machinery operated from a centralized command center rather than by factory workers physically present on the factory floor. *See Internet of Things*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/Internet_of_things [https://perma.cc/F8CJ-KJRV]; *see also* Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#14ef7da81d09 [https://perma.cc/CL8X-JA6K].

6. *See* Marr, *supra* note 4.

7. *See* Sam Judah, *What Is Skeuomorphism?*, BBC (June 13, 2013), http://www.bbc.com/news/magazine-22840833 [https://perma.cc/7H6U-7TGF]. The evolution of Apple's line of iOS devices is the prototypical example of this principle. The company has gained much attention for the way it has guided its users, teaching them to operate its then-revolutionary touchscreen devices by employing many skeuomorphic designs. By the time these devices were introduced, most consumers of technology were accustomed to using a mouse and keyboard to control their devices, so Apple had to train them to use a completely new interface. It chose to construct its mobile operating system in a way that mirrored real-life, commonplace things, allowing users to acquaint themselves with the new touch interface through familiar elements. For example, memos appeared on virtual lined yellow paper, and contacts appeared to be stored in a leather-bound book. After several years, the company released a new operating system and abandoned most of its skeuomorphism, opting, instead, for a more cutting-edge look. *See also* Kelsey Campbell-Dollaghan, *Skeuomorphism Will Never Go Away, and That's a Good Thing*, GIZMODO (Oct. 3, 2014, 1:36 PM), http://gizmodo.com/skeuomorphism-will-never-go-away-and-thats-a-good-thin-1642089313 [https://perma.cc/9357-8XQM]; Austin Carr, *Will Apple's Tacky Software-Design Philosophy Cause a Revolt?*, FAST CO. (Sept. 11, 2012, 7:45 AM), http://www.fastcodesign.com/1670760/will-apples-tacky-software-design-philosophy-cause-a-revolt [https://perma.cc/SPP5-TWME]; Clive Thompson, *Clive Thompson on Analog Designs in the Digital Age*, WIRED (Jan. 31, 2012, 12:30 PM), https://www.wired.com/2012/01/st_thompson_analog/ [https://perma.cc/EM73-VVUZ].

8. For an entertaining clip of "Today Show" anchors Bryant Gumbel and Katie Couric not understanding the Internet in 1994, see *Flashback! TODAY Anchors 'Discover' the Internet*, TODAY (Jan. 26, 2015), http://www.today.com/video/today/56868116 [https://perma.cc/MYQ4-CMSK].

9. *See* Campbell-Dollaghan, *supra* note 7; Carr, *supra* note 7; Judah, *supra* note 7; Thompson, *supra* note 7.

Interface, or "GUI"[10] — is entirely skeuomorphic.[11] The computer does not include any actual files, folders, documents, or images; there are only ones and zeros, sectors and clusters, and magnetic platters and actuator arms.[12]

Historically, however, courts have not grappled with these distinct characteristics of modern technologies and, instead, have relied too heavily upon tempting but deceptive physical analogies.[13] But computer searches are different from searches of physical locations in many ways. Most importantly, they must be conducted by trained forensic examiners who can protect the integrity of the original evidence, as well as employ specialized techniques to detect erased, protected, or otherwise-obfuscated files.[14] Objects are not merely gathered and taken off-site but are carefully processed in a scientific fashion.[15] It is a lengthy process, as the sizes of standard hard drives and the amount of data being regularly generated have grown exponentially and, therefore, take much longer to copy.[16] There are also a number of technical reasons why law enforcement conducts a bit-by-bit mirror of the source media as its regular practice.[17] Yet, rather than assess the application of the law to the actual core functioning of the relevant technologies, courts rely on seemingly obvious stand-ins that are ultimately not apropos.

---

10. *See Graphical User Interface*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/graphical_user_interface [https://perma.cc/F89V-VMWV].

11. A "skeuomorph" is "an object or feature which imitates the design of a similar artifact made from another material." *Skeuomorph*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/us/skeuomorph [https://perma.cc/Q9MB-7S7B]. In computing, the term specifically refers to "an element of a graphical user interface which mimics a physical object." *Id.*

12. *See infra* App.

13. *See, e.g.*, Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (analogizing password-protected computer files to a locked footlocker); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (analogizing the monitoring of employees' Internet use to random inspections of employees' lockers); *In re* Grand Jury Subpoena Duces Tecum, 846 F. Supp. 11, 12–13 (S.D.N.Y. 1994) (analogizing hard drives and other storage media to filing cabinets of paper documents); United States v. Chan, 830 F. Supp. 531, 534–35 (N.D. Cal. 1993) (analogizing a privacy expectation in certain electronic data to that in a personal address book); United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (equating a computer memo book with any other closed container, finding them indistinguishable and subject to the same Fourth Amendment protections).

14. *See infra* Section II.A and App.

15. *Id.*

16. *See* Hardy, *supra* note 2.

17. *See infra* Section II.A and App.

A recent case in the Second Circuit provides a clear example of when this "digital misunderstanding" inhibits the development of the law. In *United States v. Ganias*,[18] the government conducted lawful imaging of several of Stavros Ganias's hard drives, retaining full forensic copies containing data that were both responsive and non-responsive to the initial search warrant.[19] Ganias later alleged that the improper retention of the data — and, resultantly, a subsequent search three years later that was only possible because of that retention — violated his rights under the Fourth Amendment.[20] While the *Ganias* court acknowledged the limitations of the often-invoked "filing cabinet" analogy,[21] it nonetheless failed to establish the proper reasonableness standard for the search of lawfully seized digital data.[22] The case evinces the complications that arise from using pre-computer-age rules and procedures to address novel and complex technological questions. Given the revolutionary nature of today's digital landscape, this Note argues that it is unwise to attempt to force old frameworks onto non-analogous present-day situations. With digital evidence now pervading virtually every type of criminal prosecution, it is crucial to understand precisely that with which the courts are dealing and how it interacts with the Fourth Amendment.

This Note submits that, rather than adopt a clear approach in *Ganias*, thereby ensuring that the law stay apace with recent and unprecedented technological developments, the Second Circuit missed a crucial opportunity to recognize what is reasonable when searching digital data.[23] Because today's technologies are revolutionary and, therefore, fundamentally unique, they call for an entirely new framework and cannot be likened to more traditional situations with which the courts are more comfortable and familiar. Physical and digital objects have little, if anything, in common,[24] yet they are, nonetheless, conflated because technology developers use the vernacular of known real-world concepts in an attempt to lower

---

18. 824 F.3d 199 (2d Cir. 2016) (en banc).

19. *Id.* at 202–03.

20. *See* Motion to Suppress Evidence, United States v. McCarthy, No. 3:08-cr-00224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 106.

21. *See Ganias*, 824 F.3d at 212–14.

22. *See infra* Section II.B.

23. *See Ganias*, 824 F.3d at 225–26; *see also infra* Section II.B and Part III.

24. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2488 (2014) (comparing data stored on a cell phone to physical items "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.").

the learning curve for the average computer user.[25] This Note suggests that such skeuomorphic designs and elements are now leading the law astray, as mimetic details lead many — including the courts — to focus not on the functioning of the technologies themselves but, instead, on what is familiar. Consequently, the Second Circuit's analysis does a disservice by not promoting the correct law for the technology actually before it and, instead, leaving such technology vulnerable to an understanding falsely grounded in the real-life objects merely mimicked in the digital space.

Given these considerations, this Note concludes that the Second Circuit should have ruled affirmatively in *Ganias* that what the government did was facially reasonable and sufficient to satisfy Fourth Amendment requirements.[26] Instead, the court decided the case on good-faith grounds,[27] refraining from developing the law as to the complex technological questions that were presented.

This Note explores how the courts view digital information for Fourth Amendment purposes, using *Ganias* to show how the analysis can be distorted if electronic storage media are not properly understood. Part I provides context for the discussion: Section I.A recounts the facts and procedural history of Stavros Ganias's case, which resulted in a rare Second Circuit *en banc* review of his appeal; Section I.B provides a general background to relevant Fourth Amendment jurisprudence, examining the text itself, the motivation for its ratification, how courts have interpreted the warrant and particularity requirements, and the Amendment's application to computer evidence. Part II addresses the shortcomings of a non-technical analysis of digital data, highlighting the pitfalls of relying on enticing but false physical analogs. It also critiques the *Ganias* opinion for not fully embracing the realities of electronic evidence and for not defining the boundaries of reasonable computer forensic examination. Finally, Part III proposes that the issues at play in *Ganias* would be abated if courts viewed the authorized seizure as one of a physical device — a hard drive of data — rather than of the information itself, drawing several analogies to establish that no unreasonable government encroachment occurred in *Ganias* because warrants were issued by a neutral judge, agents remained within the scope of those authorities, and no reasonable expectation of privacy could, therefore, remain.

---

25. *See infra* Section II.A.
26. *See infra* Section III.B.
27. *Ganias*, 824 F.3d at 225–26.

I. STAVROS GANIAS, THE FOURTH AMENDMENT, AND COMPUTER SEARCHES AND SEIZURES

The progression of the McCarthy and Ganias investigations led to the emergence of the Fourth Amendment question with which this Note is concerned. This Part provides the necessary background for the discussion. Section I.A summarizes the factual and procedural aspects of the case. Section I.B then turns to the fundamentals of Fourth Amendment jurisprudence, with a special focus on digital searches and seizures.

A. The McCarthy and Ganias Investigations and Prosecutions

Stavros Ganias was an accountant in Connecticut.[28] Among his clients was James McCarthy, the owner of Industrial Property Management ("IPM") and American Boiler, Inc. ("AB").[29] In August 2003, government agents learned that IPM may have engaged in fraud related to an Army contract it had been awarded.[30] As part of its investigation into that misconduct, in November 2003, the government applied for and obtained warrants to search both IPM's and AB's offices.[31] In addition, the warrant authorized the search of Ganias's business, Taxes International, where IPM's and AB's financial books were maintained.[32] Agents were authorized to seize "[a]ll books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and [AB]."[33]

Because Ganias was not suspected of any crimes at that time, agents specially trained in computer forensics elected to create mirror images[34] of the three computers they discovered rather than physically remove the hard drives from the office and, thereby, significantly disrupt Ganias's business operations.[35] The images contained all of the data from Ganias's computers — not just the IPM

28. *See id.* at 201.

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. Search Warrant at 4, United States v. McCarthy, No. 3:08-cr-00224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 108.

34. A mirror image, also known as a "mirror," "image," "clone," or "bitstream copy," is an exact replica of the entirety of the media, down to every bit and byte. *See, e.g.*, BILL NELSON ET AL., GUIDE TO COMPUTING FORENSICS AND INVESTIGATIONS: PROCESSING DIGITAL EVIDENCE 37 (5th ed. 2016).

35. *Ganias*, 824 F.3d at 202 & n.6.

and AB materials — just as if the agents had seized the physical computers themselves.[36] Agents subsequently consolidated the images, archived a copy, and prepared two copies for forensic analysis, which commenced in June 2004.[37] Over the ensuing months, agents began to review the materials and identified data that were responsive to the warrant.[38] Though the agents recovered a number of files of interest to the investigation, certain materials could not be accessed and reviewed without specific proprietary software that was not immediately available to either of the computer specialists performing the search.[39] However, by December 2004, the agents were able to access the last of the digital data and reviewed the relevant IPM and AB files.[40] Based, in part, on the evidence found on the mirrors, the ongoing investigation into McCarthy, IPM, and AB culminated in the indictment of McCarthy in 2008.[41]

In the course of its McCarthy investigation and independent of Ganias's digital data that were seized pursuant to the 2003 warrant, the government officially expanded its investigation to include Ganias himself on July 28, 2005.[42] Ganias and his counsel met with the government in February 2006, at which point the government asked for consent to search Ganias's personal and business files contained on the forensic images.[43] Ganias did not respond to this request, and, in April 2006, the government sought and obtained — based on an independent showing of probable cause[44] — a warrant to search the hard drive images again, this time looking for evidence that Ganias

---

36. *Id.* at 202–03. While such a seizure may, at first glance, appear overbroad and beyond the scope of the warrant, it is necessary for a number of technical reasons. *See* discussion *infra* Section II.A and App. Courts have recognized this necessity in their interpretation of the particularity requirement of the Fourth Amendment. *See* discussion *infra* Section I.B.

37. *Ganias*, 824 F.3d at 203–04.

38. *Id.* at 204.

39. *Id.*

40. *Id.* at 205.

41. *Id.* at 205–06.

42. *Id.* at 206 n.14, 207. Agents noted potential errors in the tax returns Ganias prepared for McCarthy's companies; consequently, they subpoenaed five years of his bank records and reviewed his corresponding personal income tax returns, concluding that he might be involved in tax evasion by underreporting his own income just like he had aided McCarthy in underreporting income for McCarthy's businesses. One of the case agents testified that, once Ganias was suspected of tax crimes, the government did not look at any digital evidence pertaining to him or his business because it was not covered by the seizure authorized in the original warrant. *See id.* at 207 n.15.

43. *Id.* at 207.

44. *Id.* at 207 n.18.

had violated certain tax laws.[45] After a search of that data, Ganias was ultimately indicted for tax evasion in the same 2008 indictment charging McCarthy.[46] A superseding indictment was filed on December 21, 2009.[47]

Following motions to sever, which the court granted,[48] McCarthy agreed to plead guilty to a substitute Information[49] and was sentenced on February 4, 2011, to imprisonment for a year and a day, followed by a year of supervised release.[50] Ganias proceeded to a jury trial, which commenced on March 10, 2011.[51] The jury returned a guilty verdict on April 1, 2011,[52] and, on January 18, 2012, Ganias was sentenced to two concurrent terms of twenty-four months' incarceration, plus three years' supervised release.[53]

On the day of his sentencing, Ganias filed a Notice of Appeal from, among other things, the district court's ruling on his motion to suppress.[54] In February 2010, he had moved to suppress the evidence obtained as a result of the search of his computers pursuant to the two warrants, alleging that the warrants were overbroad and not supported by probable cause and that, therefore, the seizure, retention, and recovered evidence were the fruits of an unreasonable general warrant.[55] The district court denied the motion[56] and later

---

45. *Id.* at 207.

46. *See generally* Indictment, United States v. McCarthy, No. 3:08-cr-00224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 1. The first count of the indictment charges both McCarthy and Ganias with conspiracy to commit tax fraud under 18 U.S.C. § 371. *Id.* at 2–14. Counts Two and Three pertain specifically to McCarthy. *Id.* at 14–15. Counts Four and Five charge Ganias with violating 26 U.S.C. § 7201 (committing tax evasion). *Id.* at 15–16.

47. *See generally* Superseding Indictment, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 84. This new indictment contained the same five charges but also charged Ganias with Count Three for his role in the tax evasion related to McCarthy's individual 2003 tax return, a violation of 18 U.S.C. § 2 (aiding and abetting). *Id.* at 16–17.

48. *See generally* Ruling on Defendants' Motions to Sever, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 133.

49. *See* Plea Agreement, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 141.

50. *See* Judgment as to James L. McCarthy, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 171.

51. *See* Minute Entries, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF Nos. 182, 188.

52. *See* Verdict Form, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 215.

53. *See* Judgment as to Stavros M. Ganias, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 281.

54. *See* Notice of Appeal, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 282.

55. *See* Motion to Suppress Evidence, *supra* note 20.

56. *See* Order, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 119.

issued a written decision.[57] In its decision, the court found that: (1) the government agents seized the computer data pursuant to a valid warrant; (2) the valid warrant explicitly set forth a list of items to be seized, which included computer hardware and software; (3) the agents used less intrusive means than they were authorized to use by making mirror images of the hard drives rather than seizing and holding the computers themselves; (4) the forensic examination of the computers was conducted within the limitations imposed by the warrant; (5) the agents viewed only the relevant data that was extracted as within the scope of the warrant; (6) a copy of the evidence was preserved in the form in which it was taken; (7) the defendant never moved for the destruction or return of his data; and (8) the agents obtained the additional warrant when other leads led them to expand their investigation, which then authorized them to search additional data in their possession that they were not authorized to view under the first warrant.[58]

On appeal, the Second Circuit ordered the suppression of the digital evidence recovered pursuant to the 2006 warrant and vacated the jury verdict.[59] Although the three-judge panel was unanimous in its conclusion that the government had violated the Fourth Amendment, only two judges thought suppression was warranted.[60] The decision emphasized that a search takes place whenever the government invades persons, houses, papers, or effects or an area where a person has a reasonable expectation of privacy.[61] Similarly, property seizure occurs whenever the government interferes in a meaningful way with a person's possession of that property.[62]

However, following this initial ruling, the full court ordered rehearing *en banc*, ultimately reversing the panel and reinstating the conviction on good-faith grounds.[63] The Supreme Court denied *certiorari*.[64]

---

57. *See* Ruling on Motion to Suppress Evidence, *McCarthy*, No. 3:08-cr-00224 (EBB), ECF No. 248.

58. *Id.* at 19.

59. *See* United States v. Ganias, 755 F.3d 125, 141 (2d Cir. 2014), *rev'd en banc*, 824 F.3d 199 (2d Cir. 2016).

60. The case was before Judge Peter Hall, Judge Denny Chin, and Judge Jane Restani of the Court of International Trade, sitting by designation. Judge Chin authored the majority opinion, from which Judge Hall concurred in part and dissented in part.

61. *Ganias*, 755 F.3d at 133.

62. *Id.*

63. *See* United States v. Ganias, 824 F.3d 199, 225–26 (2d Cir. 2016) (en banc). The good-faith doctrine provides an exception to the exclusionary rule, allowing for

B. The Legal Standards for Digital Searches and Seizures

1. General Fourth Amendment Principles

The Fourth Amendment of the United States Constitution was offered and adopted in response to widespread concern about the English Crown's use of general warrants, "which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown."[65] The Amendment provides:

---

the admission of evidence collected by the police in good faith despite a defect in a search warrant or some other unlawful privacy invasion that would otherwise render inadmissible the evidence recovered. *See* United States v. Leon, 468 U.S. 897, 922 (1984) (finding that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion).

64. Ganias v. United States, 137 S. Ct. 569, 569 (2016).

65. Ashcroft v. al-Kidd, 563 U.S. 731, 742 (2011); *see also* MD. CONST. of 1776, DECLARATION OF RIGHTS, art. XXIII, *reprinted in* AVALON PROJECT, YALE LAW SCHOOL, http://avalon.law.yale.edu/17th_century/ma02.asp [https://perma.cc/F4SJ-E7YD] (finding all general warrants illegal); MASS. CONST., pt. 1, art. XIV, https://malegislature.gov/Laws/Constitution [https://perma.cc/KW3P-M4LJ] (establishing a right to be secure from unreasonable searches and seizures and finding that no warrant ought to be issued without the formalities prescribed by law); VA. DECLARATION OF RIGHTS, art. X, *reprinted in* AVALON PROJECT, YALE LAW SCHOOL, http://avalon.law.yale.edu/18th_century/virginia.asp [https://perma.cc/U9SE-27F3] (declaring that general warrants are "grievous and oppressive and ought not to be granted"); Essays of Brutus, No. II, *in* 2 THE COMPLETE ANTI-FEDERALIST 372, 375 (Herbert J. Storing ed., 1981) ("For the security of liberty it has been declared, that . . . all warrants, without oath or affirmation, to search suspected places, or seize any person, his papers or property, are grievous and oppressive." (internal quotation marks omitted)); Letters from The Federal Farmer, No. VI, *in* 2 THE COMPLETE ANTI-FEDERALIST 256, 262 (Herbert J. Storing ed., 1981) ("[H]e is subject to no unreasonable searches or seizures of his person, papers or effects . . . ."); Letters from The Federal Farmer, No. XVI, *in* 2 THE COMPLETE ANTI-FEDERALIST 323, 328 (Herbert J. Storing ed., 1981) ("[A]ll persons shall have a right to be secure from all unreasonable searches and seizures . . . and that all warrants shall be deemed contrary to this right, if the foundation of them be not previously supported by oath, and there be not in them a special designation of persons or objects of search, arrest, or seizure . . . ."); Essays by a Maryland Farmer, No. I, *in* 5 THE COMPLETE ANTI-FEDERALIST 9, 14 (Herbert J. Storing ed., 1981) ("[S]uppose for instance, that an officer of the United States should force the house, the asylum of a citizen, by virtue of a general warrant, I would ask, are general warrants illegal by the constitution of the United States? . . . Suppose a case that must and will frequently happen, for such happen almost daily in England — That an officer of the customs should break open the dwelling, and violate the sanctuary of a freeman, in search for smuggled goods — impost and revenue laws are and from necessity must be in their nature oppressive — in their execution they may and will become intolerable to a free people . . . ."). *See generally* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 79–105 (1937).

> The 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.[66]

As the language itself signals, the ultimate touchstone of the Fourth Amendment is reasonableness.[67] The Supreme Court has held that reasonableness generally requires that law enforcement obtain of a judicial warrant before searching for evidence of wrongdoing.[68] The warrant requirement ensures that any inferences supporting the search are drawn by a neutral and detached magistrate instead of by the officer "engaged in the often competitive enterprise of ferreting out crime."[69] Where law enforcement does not have a warrant, a search is reasonable only if it falls within an enumerated exception to the warrant requirement.[70] However, where the government *is* seeking a warrant, "the Warrants Clause requires particularity and forbids overbreadth."[71]

Thus, to prevent general searches, the Fourth Amendment prohibits the seizure of one thing under a warrant describing another.[72] Courts have found that, "[a]lthough somewhat similar in focus, [particularity and overbreadth] are two distinct legal issues."[73] A warrant is overbroad when there is no probable cause to support seizure of certain of the items listed.[74] A warrant is insufficiently particularized if it does not provide the executing officers with sufficient guidelines for the search.[75] Thus, breadth requires that the warrant's scope be tied to the probable cause on which the warrant is

---

66. U.S. CONST. amend. IV.

67. *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

68. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

69. Johnson v. United States, 333 U.S. 10, 14 (1948).

70. *See* Kentucky v. King, 563 U.S. 452, 459–60 (2011).

71. United States v. Cioffi, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009); *accord* United States v. Zemlyansky, 945 F. Supp. 2d 438, 450 (S.D.N.Y. 2013).

72. *See* U.S. CONST. amend. IV ("[A]nd no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized.").

73. United States v. Levy, No. S5 11 CR 62 (PAC), 2013 WL 664712, at *5 (S.D.N.Y. Feb. 25, 2013) (quoting United States v. Hernandez, No. 09 Cr. 625 (HB), 2010 WL 26544, at *7 (S.D.N.Y. Jan. 6, 2010)) (internal quotation marks omitted), *aff'd*, 803 F.3d 120 (2d Cir. 2015).

74. *See id.*

75. *Id.*

issued, while particularity requires that the warrant clearly state what is sought.[76]

In determining whether a warrant is overbroad, courts must assess whether there was probable cause to support the scope of the authorized search.[77] There is sufficient probable cause to justify the scope of the search "where the totality of circumstances indicates a 'fair probability that contraband or evidence of a crime will be found in a particular place.'"[78]

With regard to particularity, the warrant's description must be such that a typical law enforcement officer, with reasonable effort, could identify the place to be searched.[79] This Fourth Amendment requirement ensures that the search will be carefully tailored to its justifications and will not become more akin to the wide-ranging exploratory searches the Framers intended to prohibit.[80] The warrant must "describe the items to be seized with as much particularity as the circumstances reasonably allow" so as to avoid violating the Fourth Amendment by providing "no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary."[81] The particularity requirement avoids such a privacy invasion and reduces the scope of the search to what a detached and neutral magistrate has determined is supported by probable cause.[82]

---

76. *See* United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006); *In re* A Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 389 (S.D.N.Y. 2014), *as amended* (Aug. 7, 2014) [hereinafter *In re* Google Warrant].

77. *See* United States v. Zemlyansky, 945 F. Supp. 2d 438, 464 (S.D.N.Y. 2013).

78. Walczyk v. Rio, 496 F.3d 139, 156 (2d Cir. 2007) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

79. *See* Steele v. United States, 267 U.S. 498, 503 (1925); *see also* United States v. Williams, 69 F. App'x 494, 495–96 (2d Cir. 2003) ("We have previously stated the general rule regarding particularity: [i]t is enough if the description is such that the officer[s] armed with a search warrant can with reasonable effort ascertain and identify the place intended." (alteration in original) (citation and internal quotation marks omitted)); Velardi v. Walsh, 40 F.3d 569, 576 (2d Cir. 1994) (supporting the same proposition); United States v. George, 975 F.2d 72, 75 (2d Cir. 1992) ("[T]he warrant must enable the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize."); United States v. Vargas, 621 F.2d 54, 56 (2d Cir. 1980) ("[Defendant] argues that the search warrant issued by the Magistrate was insufficiently precise . . . . We agree with the court below that the description was sufficiently specific to permit the rational exercise of judgment in selecting what items to seize. The warrant did not authorize such a broad 'roving commission' as to be constitutionally offensive." (citation omitted)).

80. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987).

81. *George*, 975 F.2d at 75–76.

82. *See Garrison*, 480 U.S. at 84.

To be sufficiently particular, a warrant must contain "sufficiently particularized language that creates a nexus between the suspected crime and the items to be seized."[83] Without something clearly limiting the officers' discretion during the warrant's execution, it is meaningless to have the safeguard of a judge who reviews and approves the scope of the search in the first place.[84] For this reason, authorization to search for "'evidence of *a* crime,' that is to say, any crime, is so broad as to constitute a general warrant."[85] A mere reference to "evidence" of a violation of a general criminal statute — or just criminal activity broadly — provides no obvious guidelines for the executing officers as to what to seize.[86]

At the same time, however, generic terms may be used in describing the materials to be seized, as the Fourth Amendment does not require that each individual item or document be specifically identified in the warrant.[87] The level of specificity that is constitutionally required depends on a number of factors, including "the nature of the crime, and '[w]here . . . complex financial crimes are alleged, a warrant properly provides more flexibility to the searching agents.'"[88] To satisfy the particularity requirement, then,

---

83. Mink v. Knox, 613 F.3d 995, 1010 (10th Cir. 2010).

84. *See George*, 975 F.2d at 76; *see also Mink*, 613 F.3d at 1011 (explaining that a warrant for "all computer and non-computer equipment and written materials . . . without any mention of any particular crime" is unconstitutionally broad); United States v. Fleet Mgmt. Ltd., 521 F. Supp. 2d 436, 443 (E.D. Pa. 2007) (holding that a warrant for "any and all data" is an unconstitutionally broad general warrant); United States v. Clough, 246 F. Supp. 2d 84, 87–88 (D. Me. 2003) (finding that a warrant authorizing seizure of all text and images on the computer is unconstitutionally broad because there are "no restrictions on the search, no references to statutes, and no references to crimes or illegality"); United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (finding that a warrant for "all computers . . . all computer storage devices . . . and all computer software systems" that did not indicate "the specific crimes for which the equipment was sought" was unconstitutionally broad (alteration in original)).

85. *George*, 975 F.2d at 76 (emphasis in original).

86. *See, e.g.*, United States v. Maxwell, 920 F.2d 1028, 1033 (D.C. Cir. 1990) (wire fraud); United States v. Holzman, 871 F.2d 1496, 1509 (9th Cir. 1989) (fraud); United States v. Fuccillo, 808 F.2d 173, 176–77 (1st Cir. 1987) (stolen goods); Voss v. Bergsgaard, 774 F.2d 402, 405 (10th Cir. 1985) (conspiracy); United States v. Cardwell, 680 F.2d 75, 77 (9th Cir. 1982) (tax evasion).

87. *See* United States v. Levy, No. S511-cr-62 (PAC), 2013 WL 664712, at *5 (S.D.N.Y. Feb. 25, 2013), *aff'd*, 803 F.3d 120 (2d Cir. 2015).

88. *Id.* (quoting United States v. Dupree, 781 F. Supp. 2d 115, 149 (E.D.N.Y. 2011)); *see* United States v. Scully, 108 F. Supp. 3d 59, 90 (E.D.N.Y. 2015) (citing *Dupree* for the same proposition); *see also* United States v. Cohan, 628 F. Supp. 2d 355, 362 (E.D.N.Y. 2009) ("[T]he degree to which a warrant must state its terms with particularity varies inversely with the complexity of the criminal activity

the warrant has to be sufficiently specific to inform the executing officers' rational exercise of judgment in selecting which items to seize.[89]

In exercising that judgment, "[a]mple case authority sanctions 'some perusal, generally fairly brief, of . . . documents (seized during an otherwise valid search) . . . in order for the police to perceive the relevance of the documents to crime.'"[90] This standard is driven by the practicalities confronting the individuals executing the search, as "allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'"[91] Law enforcement must be able to exercise control over the documents as a threshold matter to determine whether they fall within the scope of the warrant.[92]

2. Searching Electronic Evidence

Regarding electronic evidence, courts have recognized that a search for responsive records cannot be completed on-site because of the enormous volume of undifferentiated information and documents, and they have thus "developed a more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness."[93] Ordinarily, the

---

investigated." (quoting United States v. Regan, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989)) (internal quotation marks omitted)).

89. *See* United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000); *see also Mink*, 613 F.3d at 1010 (finding that a warrant must state with specificity what is to be taken so that "nothing is left to the discretion of the officer executing the warrant").

90. United States v. Mannino, 635 F.2d 110, 115 (2d Cir. 1980) (quoting United States v. Ochs, 595 F.2d 1247, 1257 n.8 (2d Cir. 1979)); *accord* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); United States v. Giannetta, 909 F.2d 571, 577 (1st Cir. 1990) ("[T]he police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized."); United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981) ("The incriminating character limitation necessarily permits a brief perusal of documents in plain view in order to determine whether probable cause exists for their seizure under the warrant.").

91. United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990); *see also* United States v. Wicks, 995 F.2d 964, 974 (10th Cir. 1993) (noting that a warrant authorizing the seizure of records of criminal activity "permits officers to examine many papers in a suspect's possession to determine if they are within the described category").

92. *See In re* Google Warrant, 33 F. Supp. 3d 386, 391–92 (S.D.N.Y. 2014), *as amended* (Aug. 7, 2014).

93. United States v. Metter, 860 F. Supp. 2d 205, 214 (E.D.N.Y. 2012); *accord* United States v. Graziano, 558 F. Supp. 2d 304, 317 (E.D.N.Y. 2008) (noting that courts have afforded law enforcement "leeway in searching computers for

particularity and overbreadth requirements restrict the government's ability to seize all of someone's papers or effects for off-site examination — as items not described in the warrant are being seized, which is akin to the effects of a forbidden general, exploratory warrant.[94] However, in certain situations, the materials are so intermingled that they reasonably preclude sorting at the time of execution.[95] For instance, in response to challenges by defendants, many courts have upheld outright seizure or copying of entire hard drives — or other devices — to effectuate a proper search for whatever has been expressly specified in the warrant.[96] In *United*

---

incriminating evidence within the scope of materials specified in the warrant"); United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) ("Where proof of wrongdoing depends upon documents . . . whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant.").

94. *See supra* text accompanying notes 72–86.

95. Forensic analysis of electronic data could take many months depending on the size of the storage medium and the number of devices recovered. As such, it is simply not viable for the police to occupy a person's home or office for that length of time while determining what to seize and what to leave behind. Instead, authorities routinely create a mirror image of a hard drive, which is then searched over time in a controlled setting. *See* discussion *infra* Section II.A and App.

96. *See, e.g.*, United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013) (holding that the need to search for digital data that was not limited to a known file or set of files, as well as the inability to know how many files there were or where they might have been stored, justified the seizure and subsequent off-site search of the whole computer system); United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer haystack." (citations and internal quotation marks omitted)); United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011) (rejecting requirement of "on-site" search of hard drives because the practical realities of computer investigations preclude them); United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010) ("Undoubtedly the warrant's description serves as a limitation on what files may reasonably be searched. The problem with applying this principle to computer searches lies in the fact that such images could be nearly anywhere on the computers. Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents."); United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2006) (upholding seizure and subsequent off-site search of computer in a "laboratory setting"); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding seizure and search of an entire computer system because officers had no way of knowing where the illicit images were stored); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images [of child pornography]. A sufficient

States v. Bowen, the court found the "all records exception" to the Fourth Amendment's particularity requirement allowed for the seizure of the entirety of the defendants' email accounts and held that the Amendment did not require the warrant to specify search terms or methodologies in advance.[97] The court also found that there is no requirement that the executing authorities delegate a pre-screening function to the Internet service provider or ascertain which e-mails are relevant before copies are obtained from the Internet service provider for subsequent searching.[98] Other courts have agreed.[99]

---

chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application . . . .").

97. United States v. Bowen, 689 F. Supp. 2d 675, 681–84 (S.D.N.Y. 2010), *aff'd sub nom.* United States v. Ingram, 490 F. App'x 363 (2d Cir. 2012).

98. *Id.* at 682.

99. *See, e.g.*, United States v. Bach, 310 F.3d 1063, 1065 (8th Cir. 2002) (upholding as constitutionally reasonable the seizure of "all of the information" from defendant's email account where the service provider did not "selectively choose or review the contents of the named account"); *In re* Search of Info. Associated with [redacted]@mac.com That is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165 (D.D.C. 2014) ("[B]ecause the government's proposed procedures comply with the Fourth Amendment and are authorized by Rule 41, there is no need for Apple to search through e-mails and electronic records related to the target account and determine which e-mails are responsive to the search warrant . . . . [I]t would be unworkable and impractical to order Apple to cull the e-mails and related records in order to find evidence that is relevant to the government's investigation."); United States v. Ayache, No. 3:13-CR-153, 2014 WL 923340, at *2–3 (M.D. Tenn. Mar. 10, 2014) (denying motion to suppress "seizure of all emails in a defendant's account, where there was probable cause to believe that the email account contained evidence of a crime"); United States v. Deppish, 994 F. Supp. 2d 1211, 1219–21, 1219 n.37 (D. Kan. 2014) (noting that "nothing in § 2703 precludes the Government from requesting the full content of a specified email account, nor has the Tenth Circuit ever required warrants to identify a particularized search strategy" and concluding that such a search is not a "general search"); United States v. Lebovits, No. 11-CR-134 (SJ), 2012 WL 10181099, at *22 (E.D.N.Y. Nov. 30, 2012), *report and recommendation adopted*, No. 11-CR-134 (SJ), 2014 WL 201495 (E.D.N.Y. Jan. 16, 2014), and *report and recommendation adopted sub nom.* United States v. Gutwein, No. 11-CR-134 (SJ), 2014 WL 201500 (E.D.N.Y. Jan. 16, 2014) ("It is difficult to imagine how, as a practical matter, the government could have searched the defendants' email accounts more narrowly. Clearly, the service providers could not be expected to review and parse the emails on the government's behalf . . . ."); United States v. Taylor, 764 F. Supp. 2d 230, 236–37 (D. Me. 2011) (finding a warrant to search emails and seize evidence related to defendant's income and financial means "reasonably limits the evidence to be seized" and was not overly broad simply because the government was authorized to search all information associated with his email account); United States v. McDarrah, No. 05 CR 1182 (PAC), 2006 WL 1997638, at *9–10 (S.D.N.Y. July 17, 2006) (denying a motion to suppress the seizure of "[a]ll stored electronic mail and other stored content information" in the defendant's email account (alteration in original)), *aff'd*, 351 F. App'x 558 (2d Cir. 2009). *But cf.* United States v. Christie, 717 F.3d 1156, 1166–67 (10th Cir. 2013) (explaining that the Fourth Amendment particularity requirement may or may not

The *Bowen* court reasoned that "[t]o limit the government's computer search methodology *ex ante* would 'give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents' or other creative data concealment techniques."[100] Rather, the Supreme Court has held that the executing agents have discretion to determine how best to proceed with a search authorized by warrant.[101] The Court observed that "[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed."[102]

The 2009 amendments to the Federal Rules of Criminal Procedure added Rule 41(e)(2)(B) to reflect the case law, providing that:

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. *Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.* The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.[103]

The Advisory Committee Notes to the 2009 amendments explain that electronic storage devices contain such large quantities of data that it would be impractical for executing officers to review all of the information at the search location.[104] The Committee clarified that

---

require limitations *ex ante*, but "even if courts do not specify particular search protocol up front in the warrant application process, they retain the flexibility to assess the reasonableness of the search protocols the government actually employed in its search after the fact, when the case comes to court, and in light of the totality of the circumstances."); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("Moreover, in contrast to our discussion of the overbroad seizure claim above, there is no case law holding that an officer *must* justify the lack of a search protocol in order to support issuance of the warrant. As we have noted, we look favorably upon the inclusion of a search protocol; but its absence is not fatal.").

100. *Bowen*, 689 F. Supp. 2d at 681 (quoting United States v. Graziano, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008)); *see also* United States v. Karrer, 460 F. App'x 157, 162 (3d Cir. 2012) ("[G]iven the nature of computer files and the tendency of criminal offenders to mislabel, hide, and attempt to delete evidence of their crimes, it would be impossible to identify *ex ante* the precise files, file types, programs and devices that would house the suspected evidence."); *Stabile*, 633 F.3d at 237 ("[C]riminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, [so] a broad, expansive search of the hard drive may be required.").

101. *See* Dalia v. United States, 441 U.S. 238, 257 (1979).

102. United States v. Grubbs, 547 U.S. 90, 98 (2006) (quoting *Dalia*, 441 U.S. at 257).

103. FED. R. CRIM. P. 41(e)(2)(B) (emphasis added).

104. FED. R. CRIM. P. 41 advisory committee's note (2009).

the rule "acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant."[105] Courts have since consistently upheld this two-step procedure as explicitly authorized by the Rule.[106] As one district judge explained, "the seizure or 'off-site imaging' (that is, copying) of computer hard drives is 'a necessity of the digital era.'"[107]

Finally, there are similar impracticalities for including limitations on the timing of a search of electronic information, which would unduly restrict legitimate search objectives.[108] "The Fourth

---

105. *Id.*

106. *See, e.g.*, United States v. Kanodia, No. 15-10131-NMG, 2016 WL 3166370, at *7 (D. Mass. June 6, 2016) (explaining that, "[i]n overseeing the warrant process, the Court is 'primarily concerned with identifying what may be searched or seized—not how' and generally will not interfere with the discretion of law enforcement in determining 'how best to proceed with the performance of a search authorized by warrant'" (quoting United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) and United States v. Tsarnaev, 53 F. Supp. 3d 450, 464 (D. Mass. 2014))); Enjaian v. Schlissel, No. 14-CV-13297, 2015 WL 3408805, at *9 (E.D. Mich. May 27, 2015) ("In the Federal context, Federal Rule of Criminal Procedure 41(e)(2)(B) and its associated commentary specifically contemplates an extended search due to the existence of encryption."); United States v. Garcia-Alvarez, No. 14-cr-0621 JM, 2015 WL 777411, at *2 (S.D. Cal. Feb. 24, 2015) ("Rule 41 thus provides that electronic storage devices must be seized or copied at the site of seizure ('on-site') within the 14 days allowed for execution of the warrant, and may be copied and reviewed later at another location ('off-site'), so long as the later copying and review are consistent with the warrant."); United States v. Shah, No. 5:13-cr-328-FL, 2015 WL 72118, at *17 (E.D.N.C. Jan. 6, 2015) ("The two-step procedure which the government employed here is expressly authorized by Federal Rule of Criminal Procedure 41(e)(2)(B)."); United States v. Ulbricht, No. 14-cr-68 (KBF), 2014 WL 5090039, at *14 (S.D.N.Y. Oct. 10, 2014) ("[I]t is important not to confuse the separate concepts of the seizure of an item—which were quite specifically identified but which were seized in their entirety—with the search itself. The search is plainly related to the specific evidence sought."); United States v. Fernandez, No. 12-835 (JLL), 2014 WL 1418295, at *21–22 (D.N.J. Apr. 11, 2014) ("Defendant's argument that 'the government failed to follow the protocols set forth in the warrant for the seizure of electronic information, which mandated that a search of the materials be conducted by [a set date]' is unavailing . . . . The agents' actions here complied with the Federal Rules and were neither unconstitutional nor illegal."); United States v. Roberts, No. 3:08-CR-175, 2009 U.S. Dist. LEXIS 123188, at *43 (E.D. Tenn. Dec. 21, 2009) ("[T]he Court notes that Rule 41 has now been amended to reflect the distinction between the time the computer data is seized and the time that it is analyzed . . . .").

107. *See In re* Google Warrant, 33 F. Supp. 3d 386, 393 (S.D.N.Y. 2014), *as amended* (Aug. 7, 2014) (quoting United States v. Metter, 860 F. Supp. 2d 205, 214 (E.D.N.Y. 2012)).

108. *See id.* at 400; *see also* United States v. Burgess, 576 F.3d 1078, 1097 (10th Cir. 2009) ("Probable cause to search was unaffected by the delay and the reasons to search the computer and hard drives did not dissipate during the month and a half the items sat in an evidence locker.").

Amendment does not specify that search warrants contain expiration dates."[109]

As the foregoing discussion suggests, there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant.[110] What the Fourth Amendment requires is that the government complete its review within a *reasonable* period of time.[111] A number of cases have held that a delay of several months between the seizure and the completion of the government's review of electronic evidence is reasonable.[112] The Advisory Committee Notes indicate that "[a] substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs."[113]

---

109. United States v. Sims, 428 F.3d 945, 955 (10th Cir. 2005) (quoting United States v. Gerber, 994 F.2d 1556, 1559 (11th Cir. 1993)); *see also* United States v. Johns, 469 U.S. 478, 487 (1985) (finding that, while police officers may not indefinitely retain possession of a vehicle and its contents before they complete a valid warrantless search, the owner of the property must show that delay in the completion of a search was unreasonable because it adversely affected a privacy or possessory interest).

110. *See Metter*, 860 F. Supp. 2d at 215; *see also* United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) ("Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant . . . . The same principle applies when a search warrant is performed for documents. The documents are seized within the time frame established in the warrant but examination of these documents may take a longer time, and extensions or additional warrants are not required. The examination of these items at a later date does not make the evidence suppressible.").

111. *See Metter*, 860 F. Supp. 2d at 215.

112. *Id.* (citing United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1076–77 (D.N.D. 2008), *aff'd*, 592 F.3d 826 (8th Cir. 2010) (finding a two-month delay reasonable) and United States v. Burns, No. 07 cr 556, 2008 WL 4542990, at *8–9 (N.D. Ill. Apr. 29, 2008) (finding a ten-month delay for completion of the government's review reasonable)); *see also* United States v. Alston, No. 15 Cr. 435 (CM), 2016 U.S. Dist. LEXIS 63776, at *8 (S.D.N.Y. Apr. 29, 2016) (finding a three-month delay for the search of the defendant's iPhone to be in compliance with Rule 41).

113. FED. R. CRIM. P. 41 advisory committee's note (2009). The Committee added that, "[w]hile consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a 'one size fits all' presumptive period." *Id.*; *see also* discussion *infra* Section II.A.

Accordingly, so long as a warrant (1) specifies with particularity what evidence the government intends to seize,[114] (2) establishes probable cause that the evidence is connected to a specific criminal statute,[115] and (3) includes sufficient limitations to prevent a potential general search,[116] it meets the requirements of the Fourth Amendment.[117] For digital data, creating a mirror image of a hard drive specified in a warrant for later off-site review is constitutionally permissible in most instances — even where wholesale removal of tangible papers would not be — because of the great burdens on-site review would place on the parties.[118] Nevertheless, off-site review of the mirror images is still subject to the rule of reasonableness, as the general reasonableness standard that governs all Fourth Amendment analysis also controls the actual method of a warrant's execution.[119]

II. THE "DIGITAL MISUNDERSTANDING" AND THE IMPRACTICALITY OF *GANIAS*

Because of the way in which the average person conceives of computer data, this Note suggests that it is all too easy for the courts to impose false conceptions of what is reasonable when assessing the government's seizure and retention of a digital storage device. The *Ganias* case raises the question whether the government can keep and later use information that is acquired through the execution of a valid warrant but is beyond the scope of the initial seizure. Because responsive and non-responsive digital data are necessarily comingled, however, the government must copy or seize the entire disc, thereby seizing a great deal of non-responsive data in the process.[120] Yet, the

---

114. *See* U.S. CONST. amend. IV; *see also supra* text accompanying notes 79–89.

115. *See* U.S. CONST. amend. IV.

116. *See supra* text accompanying notes 72–78.

117. *See In re* Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Co., 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016).

118. *See supra* text accompanying notes 93–96, 103–07.

119. *See* United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant." (citation omitted)).

120. At least one commentator argues that the language of Federal Rule of Criminal Procedure 41 suggests that copying information may not be a seizure at all. *See* Mark Taticchi, Note, *Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 GEO. WASH. L. REV. 476, 488–90 (2010) (arguing that Rule 41(e)(2)(A) twice refers to seizure *or* copying and that Rule 41(f) also refers to seizures and copies as distinct alternatives). Traditionally, a seizure occurs "when there is 'some meaningful interference with an individual's possessory interests in that property.'" United States v. Jones, 565 U.S. 400, 419 (2012) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)); *see also* United

entire hard drive has been seized pursuant to a particularized warrant authorizing its seizure, and it is not unreasonable for a judge to later authorize further inquiry beyond the initial strictures of the original warrant. In determining the reasonableness of the seizure and later use, courts erroneously rely on an implicit assumption that digital data are akin to physical files. However, this Note argues that, because modern technological innovations operate fundamentally differently, they need to be treated as such by the courts, with devices — not data — subject to Fourth Amendment balancing.

A. Digital Data Only Seem Like Physical Files but Are, in Fact, Distinct

The search of a digital device is different from traditional searches of physical locations or objects in many respects. First, the ordinary police officer typically is not trained in digital forensics, which is the application of scientific methods and techniques to the search and retrieval of data from a computer hard drive or other storage medium.[121] Whereas officers routinely execute warrants and conduct

States v. Miller, 799 F.3d 1097, 1102 (D.C. Cir. 2015); Lavan v. City of Los Angeles, 693 F.3d 1022, 1027–28 (9th Cir. 2012). Some cases have held that photocopying documents or taking photographs of materials does not constitute a "seizure" because the government's actions do not meaningfully interfere with the owners' possessory interest. *See, e.g.*, United States v. Mancari, 463 F.3d 590, 596 (7th Cir. 2006) (photographs); Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992) (photographs); United States v. Thomas, 613 F.2d 787, 793–94 (10th Cir. 1980) (photocopies). At least three district courts have held that accessing or copying electronic data is not a "seizure" because such transfers do not interfere with the owner's access to or possessory interest in the data. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 719–21 (E.D. Pa. 2017); *In re* Application of the United States for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Commc'n Servs. to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009); United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *8 (W.D. Wash. May 23, 2001). This author disagrees: even though the right to exclude must — and does — yield to the needs of law enforcement, the Fourth Amendment would be meaningless if law enforcement could just copy any electronic information with no constraints. But those constraints must be reasonable under the circumstances, taking into account the realities of the digital world. *See infra* Section II.A and App.

121. *See, e.g.*, NELSON ET AL., *supra* note 34, at 2 ("The definition of digital forensics has also evolved over the years from simply involving securing and analyzing digital information stored on a computer for use as evidence in civil, criminal, or administrative cases. The former director of the Defense Computer Forensics Laboratory . . . defined it as '[t]he application of computer science and investigative procedures for legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert

physical searches, computer forensics analysis is typically performed pursuant to a search warrant by a trained analyst at a certified computer forensics laboratory.[122] Examiners employ specialized and standardized techniques and procedures when conducting their search to protect the integrity of the source evidence — the original computer or device that was seized — and to detect erased, protected, or otherwise obfuscated information.[123]

Given how hard drives work,[124] the ideal starting point for any forensic examination of digital data is the creation of a bit-by-bit copy of the source media,[125] which is then validated as an exact replica through a mathematical process known as "hashing."[126] A forensic image differs from the ordinary copying or backing up of files, as a validated acquisition tool actually creates a single "file" that contains all the data on the source disk.[127] Every bit of data from the hard drive is duplicated on a separate medium.[128] This process ensures that *all of the data* on the original hard drive is copied, not just still-existing and visible files.[129] For example, when a user deletes or

---

presentation." (second alteration in original) (citation omitted)); JOHN SAMMONS, THE BASICS OF DIGITAL FORENSICS 2 (2d ed. 2015).

122. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 71 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [https://perma.cc/H9QE-QB2Y] ("In most cases investigators will simply seize the hardware during the search, and then search through the defendant's computer for the contraband files back at a computer forensics laboratory.").

123. *See* NELSON ET AL., *supra* note 34, at 5 ("Like an archaeologist excavating a site, digital forensics examiners retrieve information from a computer or its components. The information retrieved might already be on the drive, but it might not be easy to find or decipher.").

124. *See infra* App.

125. *See, e.g.*, NELSON ET AL., *supra* note 34, at 38 ("The first rule of digital forensics is to preserve the original evidence. Then conduct your analysis only on a copy of the data—the image of the original medium."); SAMMONS, *supra* note 121, at 7 ("Examining the original media is something that should be absolutely avoided if at all possible. The danger is that the original evidence could very well be modified in some way or even destroyed outright. Preferably, a forensic image is made and all examinations are made on this duplicate, rather than the original.").

126. *See* SAMMONS, *supra* note 121, at 8. Hashing is the process by which a one-way algorithm is run across a given dataset, producing a unique value that serves as that data's "digital fingerprint" and that is used to compare two files or pieces of media to prove that they are mathematically identical. *Id.* at 61–62.

127. NELSON ET AL., *supra* note 34, at 38.

128. SAMMONS, *supra* note 121, at 54.

129. NELSON ET AL., *supra* note 34, at 38; *see also* SAMMONS, *supra* note 121, at 54 ("Why not just copy and paste the files? The reasons are significant. First, copying and pasting only gets the active data—that is, data that are accessible to the user . . . .

overwrites files on a hard drive, the disk actually still contains those deleted files and file fragments of partially overwritten files.[130] When a file is deleted by the user, the space it occupies is merely designated as free space, allowing it to be used for new or other files.[131] However, the original files remain on the disk until something else is written to the same physical location on the hard drive disk, thereby overwriting the original file.[132] Until that happens, the original files can still be retrieved, even though, from the user's perspective, those files are no longer on the computer.[133] All of this data is captured in a forensic image.[134]

Imaging and hashing are extremely important steps in the forensic process, as pressing just a single key on a running computer effects changes to its data[135] and contaminates — and potentially destroys — relevant evidence.[136] The image is created in such a way that no changes are written to the original drive[137] and it is, thus, possible to say with certainty that the mirror matches its source in all respects, including the "empty" space.[138] Therefore, part of the standard

---

Second, it does *not* get the data in the unallocated space, including deleted and partially overwritten files. Third, it doesn't capture the file system data. All of this would result in an ineffective and incomplete forensic exam." (emphasis in original)).

130. *See* NELSON ET AL., *supra* note 34, at 41.

131. *See id.*

132. *See id.*

133. *See id.*

134. SAMMONS, *supra* note 121, at 54.

135. *Id.* at 58 ("Interacting with a running computer, in any way, causes changes to the system. Any change to a piece of evidence is bad and can cause major problems from a legal standpoint. These alterations can call the integrity of the evidence into question. Even when a machine is just sitting there and powered on, things are changing. When a person interacts with a running machine, even more things are changing . . . . [T]hese changes may have no impact on the artifacts relevant to the case. But the system is changing nonetheless.").

136. *Id.* at 55 ("[D]igital evidence is extremely volatile. Thus, you never want to conduct your examination on the original evidence unless there are exigent circumstances or there is no other option available."); *id.* at 57 ("Any writes to the evidence will compromise its integrity and jeopardize its admissibility. Getting a functioning write-blocking device or software in place will keep this from happening.").

137. *Id.* at 56 ("It's *critical* to have some type of write blocking in place before starting the process. A write block is a crucial piece of hardware or software that is used to safeguard the original evidence during the cloning process . . . . The write block prevents any data from being written to the original evidence drive. Using this kind of device eliminates the possibility of inadvertently compromising the evidence." (emphasis in original)); *see also* NELSON ET AL., *supra* note 34, at 269.

138. *See* SAMMONS, *supra* note 121, at 61–62 ("A hash is a unique value generated by a cryptographic hashing algorithm. Hash values (functions) are used in a variety of ways, including cryptography and evidence integrity. A hash value is commonly

computer forensics procedure is to hash the source drive, image the drive, hash the image, and rehash the source drive to validate that the process resulted in an exact replica and that no changes were made to the original evidence.[139] Every bit of the drives — each 1 or 0 — is configured in the exact same way, making them truly identical copies.[140]

Once a duplicate has been made, forensic examiners can then use their skills, experience, tools, and knowledge of the particular investigation to attempt to locate significant artifacts on the subject media.[141] In the course of using a computer, even a savvy user will leave breadcrumbs of his activity scattered throughout the device, and this evidence can be uncovered and preserved by a forensic examiner who knows where to look.[142] This evidence is not cabined to the active files and data that the average person — or judge — contemplates when thinking about what is stored on a computer.[143] It

---

referred to as a 'digital fingerprint' or 'digital DNA.' Any change to the hard drive, even by a single bit, will result in a radically different hash value. Therefore, any tampering or manipulation of the evidence is readily detectable . . . . A hash value is sent along with the image so it can be compared with the original. This comparison verifies that the image is a bit-for-bit copy of the original."). Borrowing from and adapting Professor Sammons' example of how the slightest change will produce divergent hashes, compare the SHA1 hashes for "NYC" (02c0d1c277fbc2dd4ec90a77cea5740739c2663b) and "N.Y.C." (e1e92b5f282cde1233750126d1adc73bff2d304a).

139. *Id.* at 62. The leading forensic software, AccessData's Forensic Toolkit, or FTK, and Guidance Software's EnCase, will automatically produce hashes at each step and for each drive as part of its built-in imaging functionality. *See generally* CHRIS JENSEN, ACCESSDATA, FTK USER GUIDE (2016); GUIDANCE SOFTWARE, ENCASE FORENSIC IMAGER USER'S GUIDE (2013).

140. *See* SAMMONS, *supra* note 121, at 62. Often, a second copy is made, allowing the first copy to be archived in the same state in which it was "found" while the second copy is examined for relevant information. Yet, by retaining the "starting point" of the analysis, one can safely "start over" if something goes wrong, *id.* at 56, is able to replicate the results to verify accuracy, *id.* at 62, and has preserved a "snapshot" of the data for evidentiary purposes, *id.* It is crucial to capture and preserve the data *as it was found* on the target system. In the physical world, flipping through a book seized from someone's home will not change the contents of the book, and no one would expect an investigator to write on the original evidence or tear out a relevant page in order to return other irrelevant portions. The book would be preserved as it was found, because the integrity of the evidence is the driving consideration. However, if, after seizing the book, the officer makes a photocopy of important pages, then the investigator could manipulate and analyze those copies as needed because the original book is retained as the authentic source of the evidence. Chain of custody, as well as laying an evidentiary foundation, are both implicated.

141. *Id.* at 8.

142. *Id.* at 65–66.

143. For instance, contrary to what many people believe, deleting files does not actually do anything to the data itself—it only signals that the space occupied by

is, therefore, imperative that a forensic examination not be limited to a predetermined area and that a full image of a disk serve as the starting point, with the trained analyst looking at the whole collection of bits and bytes to determine what is relevant to the case at hand.

Professor Orin Kerr, a leading computer crime and Fourth Amendment scholar, aptly describes how computer searches "are more of an art than a science."[144] The search is an iterative process, with the forensic examiner beginning his search with simple techniques and then continuing down a different route or escalating his methods and tools based on what he uncovers.[145] The search itself informs the process, and the investigators respond appropriately.[146] For this reason, as discussed above, both case law and the Federal Rules of Criminal Procedure authorize seizure without *ex ante* limitations and permit subsequent searching subject to *ex post* review for reasonableness[147] — leaving it to the discretion of the analyst conducting the search to determine how and where to find relevant evidence within the scope of the warrant.[148] It is crucial to keep in

---

those files is available if and when the computer needs it. *See supra* notes 130–33, 257–62 and accompanying text. For a discussion of the role of the "Recycle Bin" and its forensic implications, see SAMMONS, *supra* note 121, at 73–74.

144. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547 (2005).

145. *Id.* at 575 ("[T]he computer forensics process is contingent, fact-bound, and quite unpredictable. Before an analyst starts searching a storage device, he normally has little idea which operating system the computer is running, what software is on it, how that software was used, what else is on the hard drive, or whether the suspect took steps to hide, misname, or otherwise disguise files. Perhaps the defendant made no effort to hide incriminating files; perhaps he changed file extensions, altered file headers, encrypted files, or took other steps to thwart the forensics process. Nor will investigators necessarily know what forensic tool the analyst may use when performing his search. Different forensic tools have different features; tasks that may be easy using one program may be hard using another.").

146. *Id.* ("It is difficult to know what the particular search requires and what tools are best suited to find the evidence without first taking a look at the files on the hard drive. In a sense, the forensics process is a bit like surgery: the doctor may not know how best to proceed until he opens up the patient and takes a look. The ability to target information described in a warrant is highly contingent on a number of factors that are difficult or even impossible to predict ex ante.").

147. *See supra* text accompanying notes 93–119.

148. *See* Kerr, *supra* note 144, at 545–46 ("[G]ood forensic analysis is an art more than a science. To find a specific type of file believed to be stored in a particular location or generated by a particular program, an analyst might begin by looking first at that location or program. He might run a search through known files for a particular word or phrase associated with the file or information sought. After conducting a logical search, the next step might be to try a physical search for that same string of text. The physical search would look not just in particular files, but more broadly throughout the entire hard drive.").

mind, however, that the analyst is not merely sorting discrete files into "relevant" or "irrelevant" categories, as the average computer user may when organizing his electronic data or as an officer does when conducting a traditional physical search.[149] The examiner is conducting a *forensic* search, and the whole hard drive, as one seized entity, is the subject of the review and can shed light on the case.[150]

B. The Shortcomings of the *Ganias* Opinions

Given the serious and complex considerations that pertain to digital searches, this Note argues that the Second Circuit should have reached the Fourth Amendment question and found that the government's actions were facially reasonable and constitutionally sufficient. In November 2003, the government sought and obtained a warrant for a distinct investigation based on particularized facts.[151] Based on the investigation and various pieces of collected evidence, the government responded to its increased knowledge, adapting and reacting to what the facts revealed. As such, Ganias was officially named a subject of the investigation in July 2005 — which he had not been when the investigation commenced and when his hard drives were imaged.[152] The investigation continued to unfold organically, but when, after several months, Ganias did not respond to the government's request that he consent to its search, the agents obtained a second judicially authorized search warrant at the end of April 2006.[153] This natural progression, with court involvement along the way, should hardly be described as an unreasonable search and seizure; rather, the government diligently worked to uncover criminal activity and to build a successful prosecution — ultimately with great success.

---

149. *See infra* App.; *see also* Kerr, *supra* note 144, at 544 ("In contrast to physical searches, digital evidence searches generally occur at both a 'logical' or 'virtual' level and a 'physical' level. The distinction between physical searches and logical searches is fundamental in computer forensics: while a logical search is based on the file systems found on the hard drive as presented by the operating system, a physical search identifies and recovers data across the entire physical drive without regard to the file system.").

150. *See infra* App.; *see also* Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 127 (2011) ("Another problem with the file strategy is its underlying assumption that only files contain evidence. That assumption is a gross simplification. Forensic examiners examine media, not just files.").

151. *See* United States v. Ganias, 824 F.3d 199, 201 (2d Cir. 2016) (en banc).

152. *See supra* note 42.

153. *See Ganias*, 824 F.3d at 207.

Had the government decided to include Ganias as a target of the investigation the day after the original seizure of his data, would the "retention" (for a day) and re-search of the materials pursuant to a new warrant be considered unreasonable? Conversely, had the government never focused on Ganias but, two-and-a-half years later, found a new piece of relevant evidence as to McCarthy on the hard drives, would it be unacceptable for the government to continue exploiting what it lawfully possessed to strengthen its initial investigation? It would be hard to object to these hypotheticals, so it is unclear why, when looking through evidence for Investigation One and finding a lead for Investigation Two, the government should not be allowed to expand the scope of its initial search through a new warrant, allowing it to pursue both investigations. Moreover, the McCarthy prosecution was still pending, so it was not unreasonable to retain the seized hard drive so it could serve as relevant evidence. Therefore, if the government reasonably possesses a lawfully seized hard drive, why should it not be able to obtain an additional warrant from the court, expanding the boundaries of the search?

Additionally, here, Ganias moved to suppress the evidence while he was being prosecuted.[154] It was this motion that led to the appeal and rehearing *en banc*. But, had he never become the subject of an investigation, the retention of the data for the investigation and prosecution of McCarthy would not have been challenged as unreasonable. While there is an underlying concern about general warrants, questions about the propriety of the search and seizure only arose because irrelevant information suddenly became relevant when the investigation was broadened to include an additional subject. Even then, the agents proceeded as they should, obtaining a particularized warrant at each step of their investigation.

Not only are Ganias's arguments unfounded, but the solution he demanded is not viable. Ganias argued that considerations underlying the prohibition on general warrants may require that, when the government lawfully images an entire hard drive — containing both responsive and non-responsive information — for off-site review, it may not retain the mirror throughout the pendency of the investigation.[155] However, there is no other forensically sound manner by which to preserve digital evidence in an investigation.[156] The responsive and non-responsive data are inextricably linked

154. *See* Motion to Suppress Evidence, *supra* note 20.
155. *See id.*
156. *See supra* text accompanying notes 124–50.

because of how they reside on the storage medium.[157] Some cannot be taken while leaving the rest behind,[158] and, at the early stages of an investigation, what can be found — or a clear distinction between what is relevant or irrelevant — may not even be known.[159] Therefore, it would be foolish to, in effect, corrupt the evidence[160] when the full range of potential evidence has not yet been identified,[161] as the process of hastily plucking a single obviously pertinent file could result in overwriting less obvious data that is harder to retrieve but that would be highly probative if uncovered. The interwoven whole must be taken in its entirety,[162] with the data therein carefully parsed — pursuant to the scope of the warrant — for use as evidence.

The Advisory Committee's comment to the 2009 amendments to Federal Rule of Criminal Procedure 41(e)(2)(B) recognizes the need for a two-step process — seizing/copying the entire storage medium and later reviewing it to determine what electronically stored information falls within the scope of the warrant — because computers and other electronic storage media commonly contain such large amounts of information that it is impractical, if not impossible, for law enforcement to review all of the information during the execution of the warrant.[163] Thus, apart from the effects of the ways in which the individual bits of datum interact, the whole should be seized because attempts to parse the information before seizure would be unworkable and inefficient in light of the sheer volume of information.[164] This explains why the warrant itself authorized the

157. *See infra* App.

158. *Id.*

159. *See* Kerr, *supra* note 144, at 575; *see also* Goldfoot, *supra* note 150, at 140–41 ("Searching for electronic evidence is like looking for needles in a haystack. If an officer looks for a needle in a haystack, he must look at a lot of hay. Worse, if he doesn't know how many needles there are, but must find all of them, then he must look through *all* the hay.").

160. *See* SAMMONS, *supra* note 121, at 55, 57, 58; *see also infra* App.

161. *See* Kerr, *supra* note 144, at 575.

162. *See* Goldfoot, *supra* note 150.

163. *See supra* text accompanying notes 103–13.

164. *Id.* As noted above, courts have applied and generally accepted this same two-step process for email search warrants for the same reason. *See supra* text accompanying notes 97–100. In these instances, the warrant acts as a twofold instrument: an order requiring the provider to turn over data in its possession and an order permitting a government agency to review those materials. *See* 18 U.S.C. § 2703(a), (d) (2018). Given that the provider has no knowledge of the investigation and what is relevant or not, it merely turns over the entirety of the content it has; the government then reviews and finds what it needs in that mass of data. *See, e.g.*, *In re* Search of Info. Associated with [redacted]@mac.com That is Stored at Premises

seizure of the hard drive, not just specific files that might be found on it.[165]

To support his motion to suppress the evidence, Ganias relied on *United States v. Tamura*, a Ninth Circuit case in which physical records were seized and later sorted into responsive and non-responsive items.[166] There, it was clear that papers outside the scope of the warrant were seized and retained in violation of the Fourth Amendment.[167] However, while not actually making a determination because of its good-faith resolution, the *Ganias* court noted in dictum that *Tamura* is different because, in *Ganias*, the 2003 warrant specifically authorized the agents to seize hard drives and to search them off-site — a key difference that distinguishes *Ganias* because the agents did not come into possession of anything unlawfully.[168] In *Tamura*, the initial seizure was not warranted[169]; the officers seized for off-site review records that the warrant did not authorize them to seize and retained those records even after their return was requested.[170] In contrast, in *Ganias* the question was whether, at

---

Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165 (D.D.C. 2014) ("[I]t would be unworkable and impractical to order Apple to cull the e-mails and related records in order to find evidence that is relevant to the government's investigation."); United States v. Lebovits, No. 11-cr-134 (SJ), 2012 WL 10181099, at *22 (E.D.N.Y. Nov. 30, 2012), *report and recommendation adopted*, No. 11-cr-134 (SJ), 2014 WL 201495 (E.D.N.Y. Jan. 16, 2014), and *report and recommendation adopted sub nom.* United States v. Gutwein, No. 11-cr-134 (SJ), 2014 WL 201500 (E.D.N.Y. Jan. 16, 2014) ("Clearly, the service providers could not be expected to review and parse the emails on the government's behalf."). The extent of the provider's role is that it can say what was requested of it, whether it had records matching that request, and that, if so, it turned those materials over to the government. The provider can only speak to the overall production it passes along. Another witness would need to articulate what is relevant and verify that it was found within the data he or she was provided—something the provider would have no way of knowing. The same is true for the mirror files created when imaging a device; the process does not involve copying all of the individual files (as an average computer user may) but actually involves creating one massive file that stands alone and that is then handed off for individual threads to be pulled from the larger weave.

165. *See* Search Warrant, *supra* note 33, at 3–5. Having seized a coherent piece of evidence, it is clear that its retention for use as evidence is reasonable. *See infra* Part III.

166. United States v. Tamura, 694 F.2d 591, 594 (9th Cir. 1982).

167. *Id.* at 596 ("In the absence of an exercise of [a neutral, detached magistrate's] judgment prior to the seizure . . . it appears to us that the seizure, even though convenient under the circumstances, was unreasonable.").

168. *See* United States v. Ganias, 824 F.3d 199, 211 (2d Cir. 2016) (en banc).

169. *See Tamura*, 694 F.2d at 595 ("It is highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the fourth amendment.").

170. *Id.* at 595–97.

some point, the retention of what was lawfully seized suddenly became unreasonable, especially when its return was never requested.[171] In *Ganias*, there is no question that the government was entitled to seize the materials it did; the issue was whether it had the right to retain that data and subsequently re-search it.

In addition, *Tamura* is inapposite because that case involved paper records and, therefore, did not account for the complexities of modern technology; such analogies that seem to apply on the surface are not appropriate at all.[172] There is a strong temptation to adopt familiar stand-ins for complex technological issues, but that superficial appeal must be overcome.[173] The court, however, failed to "decide the relevance, if any, of *Tamura*" and instead resolved the case on good-faith grounds.[174]

The court stated that it must be attuned to "the technological features unique to digital media as a whole and to those relevant in the particular case."[175] Why, then, did it not rule on what is reasonable and squarely address the novel technological features themselves? The opinion argued that it raised the privacy question, the aptness and limitations of Ganias's analogies, and the government's concerns to highlight the intricacy of the questions for future cases and to underscore the importance of engaging with the technological specifics in answering such questions.[176] But, if so, why wait and not just resolve it now? The opinion justified its approach, writing, "Caution, although not always satisfying, is sometimes the most appropriate approach."[177] Here, however, caution offers no consensus or guidance and will only result in more confusion. In *New York v. Belton*, the Supreme Court had articulated that "[a] single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront."[178] Similarly, as Judge Calabresi previously noted in his

171. *See Ganias*, 824 F.3d at 203 n.7, 207, 211.

172. *See supra* Section II.A and *infra* App.

173. *See supra* Section II.A and *infra* App.

174. *Ganias*, 824 F.3d at 211.

175. *Id.* at 213.

176. *Id.* at 217.

177. *Id.* at 221 n.42.

178. New York v. Belton, 453 U.S. 454, 458 (1981); *see also* United States v. Chadwick, 433 U.S. 1, 22 n.3 (1977) (Blackmun, J., dissenting) ("A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions, may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be

concurrence in *United States v. Cancelmo*, courts of appeal typically have the final word in the vast majority of cases in which good faith supplants the need for a probable cause finding.[179] He explained:

> This means that we owe a duty to define the boundaries of probable cause, so that affiants submitting applications for warrants, issuing magistrates, reviewing courts, and the executing officers on whose good faith we rely may have appropriate guidance. And these boundaries are best set, not by abstract statements, but by case-by-case decisions in real situations.[180]

Yet, by making a finding of good faith and not reaching the merits of the Fourth Amendment question in *Ganias*, the Second Circuit has only further complicated an already complex space. The court has not clarified the constitutionality of these technical searches. This silence raises a number of difficult questions. If the same facts play out today in an entirely separate case, would the investigating agents be entitled to rely on a warrant in good faith? If no court has answered the question, should we expect the agents to do so? Should a reviewing magistrate think twice before issuing a warrant for data that have already been in the government's possession for some time? Does it matter whether the new evidence relates to the same case or defendant for which the original warrant was issued? The court explained that no court had held that the retention of a mirrored hard drive during the pendency of an investigation would violate the Fourth Amendment.[181] Yet, that statement still holds true today, as the court failed to resolve the issue one way or the other.

As the court suggested, perhaps a statutory provision could serve as a guide.[182] Under this rubric, a determination of whether retention is still necessary would be made by the trial court on a motion from the person whose property has been seized, according to Federal Rule of Criminal Procedure 41(g).[183] Yet, the Second Circuit declined to

---

literally impossible of application by the officer in the field." (internal quotation marks omitted)).

179. *See* United States v. Cancelmo, 64 F.3d 804, 809 (2d Cir. 1995).

180. *Id.*

181. *See Ganias*, 824 F.3d at 225.

182. *See id.* at 220 ("In acknowledging the role of Rule 41(g), then, we seek also to suggest that search and seizure of electronic media may . . . merit not only judicial review but also legislative analysis; courts need not act alone.").

183. The rule provides: "A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose

rule on the factors that should be considered and offered no clear pathway for the lower courts that will have to grapple with motions regarding property retention and return. The court noted that, because it resolved this case on other grounds, it "need not address whether Ganias' failure to make such a motion forfeited any Fourth Amendment objection he might otherwise have had to the Government's retention of the mirrors."[184] With some guidance, the trial courts, perhaps, would be best suited to determine whether the seized materials were still needed for the many reasons discussed above. The court, however, provided little direction to those courts because it did not rule on the ultimate question — whether the retention of forensic copies of hard drives during the pendency of an investigation violates the Fourth Amendment.

As discussed,[185] the Advisory Committee noted that Rule 41(e)(2)(B) does not create a presumptive uniform time period within which off-site review must take place,[186] so *the court* should be afforded deferential review of its findings as to the reasonable circumstances of the retention. This approach would safeguard privacy interests — through a motion to the trial court — while also addressing the needs of law enforcement given the challenges posed by technological changes.[187] If the court denies the motion and, in essence, re-authorizes the government to possess what it lawfully seized, then subsequent law enforcement activity, such as obtaining and executing a new warrant for newly identified relevant portions of the data, would also be lawful. However, because the Second Circuit, after electing to rehear the matter *en banc*, articulated no precedential guidance as to the retention question, it lends no assistance to future courts facing similar issues — only fueling legal complications pertaining to computers and digital data. None of the

---

reasonable conditions to protect access to the property and its use in later proceedings." FED. R. CRIM. P. 41(g).

184. *Ganias*, 824 F.3d at 219.

185. *See supra* text accompanying notes 103–13.

186. FED. R. CRIM. P. 41 advisory committee's note (2009).

187. *Id.* ("It was not the intent of the amendment to leave the property owner without an expectation of the timing for return of the property, excluding contraband or instrumentalities of crime, or a remedy. Current Rule 41(g) already provides a process for the 'person aggrieved' to seek an order from the court for a return of the property, including storage media or electronically stored information, *under reasonable circumstances*. Where the 'person aggrieved' requires access to the storage media or the electronically stored information earlier than anticipated by law enforcement or ordered by the court, *the court on a case by case basis can fashion an appropriate remedy, taking into account the time needed to image and search the data and any prejudice to the aggrieved party*." (emphasis added)).

issues raised by *Ganias* has been answered, yet those issues are sure to resurface again and again.

Unlike the majority, the dissent did reach the issue and at least put forth clear — albeit mistaken — law. The *en banc* opinion overrode the bright-line pronouncement of the original panel opinion, which, though flawed, was not replaced with anything more suitable. The dissent suggested that "[the government] argues that when computers are involved, it is free to overseize files for its convenience, including files outside the scope of a warrant, and retain them until it has found a reason for their use."[188] However, as discussed, the government's actions were not undertaken for convenience but out of necessity.[189] If it were merely concerned about convenience, the government could have saved itself the effort of imaging onsite and would have simply seized all of the original hard drives as the warrant authorized it to do,[190] inconveniencing Ganias but vastly expediting its fieldwork. The government was not asking for greater latitude, as the dissent claimed,[191] but rather was treating a totally different scenario as necessitating a new framework, as the seizure and search of electronically stored information does not lend itself to the strictures suggested.

With respect to authenticating the data at trial, the dissent minimized the implications of losing an unchangeable baseline snapshot, writing that, "[a]s a practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image."[192] But this fails to recognize that, without being able to point to the original source location on the bit-for-bit copy, it would just be the witness' word that specific digital evidence came from where he says it did. Even though the defendant retained the original and the government analyzed an image, the forensic examiner would still explain (and provide documentation regarding) from where the relevant digital evidence came — the precise benefit of an exact bit-for-bit copy. The exactness of identical duplicates can be clearly shown.[193]

However, were select files extracted and no original source retained, there would be no way to go back and verify the findings in

188. *Ganias*, 824 F.3d at 226 (Chin, J., dissenting).
189. *See supra* text accompanying notes 124–50.
190. *See* Search Warrant, *supra* note 33, at 3–5.
191. *See Ganias*, 824 F.3d at 226 (Chin, J., dissenting).
192. *Id.* at 235.
193. For a discussion of hashing, see SAMMONS, *supra* note 121, at 8, 61–62.

advance of or during testimony about digital evidence. All of the findings in a forensic report point back to the precise locations on the original drive where the items discovered were located. So, by having a forensic report and the original image, anyone can use the report as a roadmap to recheck the forensic examination and validate or discredit the findings and testimony. If there is no source, however, it comes down to the witness' testimony alone, constricting the defense's ability to attack the specifics but also leaving the government's case vulnerable to distortion that cannot be rebuffed. For example, retention is necessary because the government may need to respond to defenses raised about the data on cross-examination. This could involve reexamining something already looked at, searching for something not yet uncovered, or even trying to prove that something, in fact, *did not* happen. To prove a negative, the examiner would need to be able to look at the entirety of the drive and confirm that the absent thing is not located anywhere whatsoever on the drive.[194] Defense counsel could also make claims

194. A frequent defense is that a virus affected the defendant's computer and surreptitiously downloaded the incriminating evidence (such as images of child pornography or stolen personal identifying information). In some instances, the government examiner might go back and look at the drive image and conclude that there was no virus located anywhere on the hard drive. Similarly, the examiner may go back and search for viruses (which might not have been relevant originally and, therefore, not discussed in his findings) and, finding some, opine on the validity of the defendant's claim. *See, e.g.*, United States v. O'Keefe, 461 F.3d 1338, 1341 (11th Cir. 2006) ("[The government's expert] testified that the two viruses he found on [the defendant's] computer were not capable of 'downloading and uploading child pornography and sending out advertisements.'"); *see also* Goldfoot, *supra* note 150, at 141 ("Sometimes the crucial evidence is 'the dog that did not bark[]' . . . —the absence of evidence that would be present if something happened, thus suggesting it did not happen. If a defendant claims he is innocent because a computer virus committed the crime, the absence of a virus on his hard drive is 'dog that did not bark' negative evidence that disproves his story. If a defendant claimed he sent an e-mail but it cannot be found on his hard drive, that absence is also 'dog that did not bark' negative evidence. To prove something is not on a hard drive, it is necessary to look at every place on the drive where it might be found and confirm it is not there."). In fact, Ganias himself made such a claim. *See Ganias*, 824 F.3d at 207 n.16 ("According to Agent Hosney, in that proffer session Ganias claimed 'that he failed to record income from his own business [to his QuickBook files] as a result of a computer flaw in the QuickBooks software . . . [but that,] . . . although he attempted to duplicate the software error, he was unable to do so.' Agent Hosney contacted Intuit, Inc., which released QuickBooks, to determine whether such an error might have affected, generally, the pertinent version of the software, and was told that the company was aware of no such 'widespread malfunction.'" (alterations in original) (citations omitted)); *id.* at 214 n.31 ("Data confirming the existence, or non-existence, of an error affecting the particular installation of a program on a given digital storage device could be, in a hypothetical case, relevant to the probity of information otherwise located thereupon.").

of tampering, so the government needs to have the ability to go to the full image, verify that it has not changed from its original state, and demonstrate the source of the relevant data it is using. By retaining the original source evidence, a full chain of custody can be established and the evidence can be definitively authenticated.[195]

Finally, retention of the full copy of a hard drive is necessary to safeguard the defense's ability to present its case. The government must be able to provide the defendant with a copy of what it plans to use against him.[196] As discussed, digital information is volatile, so even if the defendant retained the original device the whole time — as was the case in *Ganias* — the information would not be the same the moment the device is next used, even if the relevant data were still present at the time of trial[197] — which was not the case in *Ganias*. If a defendant is going to hire his own forensic specialist to attempt to rebut the allegations being leveled against him, that person needs to be able to conduct his examination from the same starting point as the government, with the same file remnants and residue interspersed in and among the visible files.[198] The defense may also be interested in looking for exculpatory evidence or other information on the drive that the government did not view as significant, making it unfair for the defendant if he only gets to see what the government has chosen to extract as relevant to its case.[199] Here, as before, the dissent dismissed the need to retain a copy for evidentiary purposes, saying that "[t]he Government is essentially arguing that it must hold on to

---

195. Investigators will routinely testify that they seized a digital device from a specific location and provided it to a specific person or unit. Then the forensic examiner will testify that he or she obtained the device from the investigator or an evidence locker and, after imaging it, conducted various examinations of that data. Seizure details, hash values, and other pertinent information are all logged and reported. If the original evidence is not retained in full, then there is a missing piece in the chain when presenting the case to a jury, which defendants would undoubtedly use to their advantage.

196. *See* FED. R. CRIM. P. 16(a)(1)(E).

197. *See supra* text accompanying notes 135–40. For instance, if the government searched a computer, found and seized a relevant spreadsheet for use as evidence of the charged crime, but then gave back the computer, even if the spreadsheet were still present at the time of trial, the metadata and other associated information would have changed.

198. *See, e.g.*, United States v. Kimoto, 588 F.3d 464, 480 (7th Cir. 2009) (discussing how defense experts argued "that the discovery provided to the defense did not appear to be a complete forensic copy, and that such was necessary to verify the data as accurate and unaltered").

199. Unlike the dissent, the majority recognizes that such considerations are relevant and not trivial. *See Ganias*, 824 F.3d at 215 n.35.

the materials so that it can give them back to the defendant."[200] However, as discussed, this is a drastic oversimplification of the factors at play, and the government's concerns are not obviated "simply by returning the non-responsive files to the defendant in the first place."[201] The dissent's reasoning exemplifies the temptation of the "digital misunderstanding," reaching the wrong outcome because of how the issues were framed.

III. *GANIAS* SIMPLIFIED IF VIEWED FROM A DIFFERENT PERSPECTIVE

It is important to understand: data on a hard drive is actually one thing — a magnetic platter containing interwoven information that, taken together, comprises the documents, images, and software with which users regularly interact.[202] Ordinarily, data from multiple locations come together to form what *the user* sees as a single file; but it is the whole drive, both the active data and the latent information in previously-used or empty space, that can inform an investigation and that is the actual evidence.[203] Therefore, a hard drive must be understood as and treated like a single entity, protected as such to make sure that no accidental changes are made, which could overwrite relevant information.[204] By design, hard disks themselves are fragmented, with information rarely stored in one place in case of hardware failure.[205] In fact, a single file can be stored across entirely separate hard drives.[206] Thus, unlike physical files in a folder,

200. *Id.* at 235 (Chin, J., dissenting).

201. *Id.*

202. *See infra* App.

203. *See supra* Section II.A.

204. *See supra* text accompanying notes 135–40.

205. Hard drives can be divided into partitions, which specify how much of the hard drive a given file system can occupy. The hard drive itself will start with a Master Boot Record, which has a partition table identifying how the drive has been divided and identifying the starting and ending sectors of each partition. Partitions can also be divided into smaller virtual partitions, and a computer can have multiple hard drives. Thus, the device can be configured in a number of ways, and each partition can be formatted with any file system (for example, a single hard drive can contain one partition running Windows and another partition running Linux or Mac OS). *See* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 450–52 (3d ed. 2011).

206. For example, with a RAID, or a "redundant array of independent disks," multiple physical hard drives are configured to act as a single logical drive. In other words, the data is spread across a number of disks to improve both redundancy and performance. However, the entire array appears to the operating as a single logical hard disk. *See RAID*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/us/raid [https://perma.cc/2RZE-HPYJ]

computer data cannot be neatly segregated into responsive and non-responsive data upon first review. Forensic examinations of digital data are iterative processes, and it may take several passes and varying levels of tools and techniques to extract just some of the wealth of relevant information that may be hidden in the haystack of a single hard drive.[207]

Thus, because of features that simply do not exist in the context of paper files, it is important to try to avoid the trap of speciously analogizing rather than viewing digital issues in their own right. The government's search or seizure of digital media cannot be constrained by the limitations historically imposed on physical searches, as the realities of modern technologies are wholly different and should not be governed by procedures that significantly and unduly cabin the government's legitimate enforcement efforts. Whenever digital data are searched, a neutral judge will have issued a warrant for a particular hard drive based on specific probable cause, which should obviate concerns about haphazard governmental rummaging and widespread, invasive general searches. As such, when the government obtains a digital device pursuant to a warrant, it is inherently reasonable that it retain the whole drive through, at a minimum, the pendency of the investigation and prosecution — especially when it can be demonstrated that fruitful evidence has been found therein.

A. Better, but Less Obvious, Analogies that Support the Authority To Retain and Search

Josh Goldfoot, Deputy Chief of the Computer Crime and Intellectual Property Section of the Department of Justice, persuasively argues that, although search and seizure law is the product of a number of authorities over different periods of time, with few exceptions, the authors all assume "an external, physical

---

("Redundant array of independent (or inexpensive) disks, a system for providing greater capacity, faster access, and security against data corruption by spreading data across several disk drives.").

207. *See* Kerr, *supra* note 144, at 544 ("Computer searches tend to require fewer people but more time. According to Mark Pollitt, former Director of the FBI's Regional Computer Forensic Laboratory Program, analysis of a computer hard drive takes as much time as the analyst has to give it. If the case is unusually important or the nature of the evidence sought dictates that a great deal or a specific type of evidence is needed, the analyst may spend several weeks or even months analyzing a single hard drive. If the case is less important or the nature of the case permits the government to make its case more easily, the investigator may spend only a few hours.").

perspective."[208] As such, search and seizure rules apply to *physical* objects. With technology, attempts to subdivide and differentiate between the abstract data and their tangible representations on some storage medium is, therefore, misplaced.[209] Digital evidence is ultimately just a physical manifestation of abstract information that cannot actually exist apart from its physical reduction. Thus, a physical thing — the storage medium itself — is seized, not the information thereon. Were the government to seize a single piece of paper with both responsive and non-responsive information on it, it would be unreasonable to expect the government to tear off the non-responsive parts and hand them back. By recognizing a seized drive of digital data as a cohesive entity, the treatment of digital evidence is much clearer, and the seizure of such evidence is regulated by a reasonableness inquiry that is closer to that used for other physical evidence.[210] Seen in this light, the complexity of the *Ganias* issue diminishes and the correct result becomes apparent: having lawfully seized the hard drive and still requiring it for the investigation, it is perfectly reasonable for the government to seek and obtain judicial authorization to also use the hard drive for another purpose. As long as authorities are in lawful possession of the evidence as part of an ongoing investigation or prosecution, they should be permitted to pursue any lawful avenues for further investigation of the same or an otherwise-related matter.

The reasonableness of this approach will be demonstrated by way of three analogies that are more apropos than the tempting and often invoked "filing cabinet" comparison, which does not account for the realities of the technology — making the analogy a poor fit.[211] While no analogies are perfect because of the uniqueness of the technological questions before the courts, a lot can be gained by not looking to subdivide the seized evidence fictitiously. What is seized is a hard drive of digital data; it should be preserved, maintained, and evaluated just like most other types of physical evidence that could be recovered.

---

208. Goldfoot, *supra* note 150, at 122.

209. *See, e.g.*, People v. Aleynikov, 48 N.Y.S.3d 9, 15–17 (App. Div. 2017) (finding that the electronic transmittal of stolen proprietary source code constituted a tangible reproduction since it necessarily took up physical space and was physically present on a physical hard drive), *aff'd*, 104 N.E.3d 687 (N.Y. 2018).

210. *See* Goldfoot, *supra* note 150, at 149.

211. The *Ganias* court recognizes the potential imperfection of the filing cabinet analogy and vaguely references possible alternatives; however, the opinion fails to address them thoroughly or to adopt the implications of those better comparisons as a holding. *See* United States v. Ganias, 824 F.3d 199, 212–13 (2d Cir. 2016) (en banc).

1. Seizure of a Car

There are a number of reasons why the police may seize a person's car. For instance, if a vehicle is used in or to facilitate the commission of a crime, it can be seized as an instrumentality of the crime.[212] A car may also be seized because it threatens safety or presents traffic hazards.[213] Often when such a seizure occurs, the police are authorized to conduct a search without a warrant.[214] For the sake of this argument, however, suppose that the police seize an automobile pursuant to a warrant because they have sufficient probable cause to believe that it was involved in a fatal hit-and-run accident. The police execute the warrant, recover the car, and bring it to an evidence garage for examination and safekeeping. Suppose they swab the bumper to look for evidence of the victim's DNA and, when the tests come back, they confirm that the police found exactly what they thought they did: direct evidence of the defendant's wrongdoing. Would the retention of the evidence for the pendency of the

---

212. *See, e.g.*, Cooper v. California, 386 U.S. 58, 62 (1967) (affirming the search of petitioner's impounded vehicle and subsequent seizure of evidence as reasonable because it was closely tied to the reason petitioner was arrested, the reason his car was impounded, and the reason why it was retained—transporting narcotics); Van Oster v. Kansas, 272 U.S. 465, 469 (1926) (affirming forfeiture of defendant's vehicle due to its use in the illegal transportation of liquor).

213. *See, e.g.*, South Dakota v. Opperman, 428 U.S. 364, 375–76 (1976) (finding an inventory search of a car that was impounded for minor parking violations to be reasonable given the police's caretaking function); Cady v. Dombrowski, 413 U.S. 433, 441 (1973) ("Local police officers, unlike federal officers, frequently investigate vehicle accidents in which there is no claim of criminal liability and engage in what, for want of a better term, may be described as community caretaking functions, totally divorced from the detection, investigation, or acquisition of evidence relating to the violation of a criminal statute."); Breath v. Cronvich, 729 F.2d 1006, 1008 (5th Cir. 1984) (finding a statute that permitted police to impound illegally parked vehicles constitutional); Sutton v. City of Milwaukee, 672 F.2d 644, 646 (7th Cir. 1982) (holding that pre-seizure notice and a hearing are not required when the impounded vehicle is illegally parked but not blocking traffic or otherwise creating an emergency); Commonwealth v. Gatlos, 76 A.3d 44, 47–48 (Pa. Super. Ct. 2013) (finding impoundment of the vehicle after a crash lawful and the subsequent search reasonable as an inventory search); State v. Bales, 552 P.2d 688, 689 (Wash. Ct. App. 1976) ("Reasonable cause for impoundment may, for example, include the necessity for removing (1) an unattended-to car illegally parked or otherwise illegally obstructing traffic; (2) an unattended-to car from the scene of an accident . . . (3) a car that has been stolen or used in the commission of a crime when its retention as evidence is necessary; (4) an abandoned car; (5) a car so mechanically defective as to be a menace to others using the public highway . . . .").

214. The body of law pertaining to vehicle searches and seizures is vast and complex in and of itself. Rather than address all the nuances and factors at play in that area, this argument will assume that warrants were necessary for and obtained prior to the hypothetical searches.

investigation and potential trial be reasonable? Would anyone expect the government to return, say, the seats, radio, and seatbelts because they are not relevant to the case and, therefore, should be considered unlawfully over-seized and beyond the scope of the warrant?

To take the comparison one step further, suppose the police independently realize that the car they have seized appears to be one in which they have been interested for a separate investigation into a gang-related shooting. It is the big break in an investigation that had stalled. Now the police prepare a new affidavit laying out the probable cause for their need to search the car for a new type of evidence. A judge reviews the facts and authorizes the warrant. In the course of their new search, the police find a hidden trap[215] containing several illegal firearms — direct evidence incriminating their second suspect. Should this evidence, only found because the police happened to have made the seizure in the course of their initial investigation, be suppressed? There is an aspect of bad luck for the second defendant, but does that mean that the government's actions violated the Fourth Amendment? Particularized warrants were executed, and fruitful results were recovered from appropriately limited searches.[216] The mere fact of retention should not render the process unreasonable.

Finally, now imagine that either of the defendants — the hit-and-run driver or the gang shooter — raises some claim or defense at trial. Might the government need to go back and perform additional searches or analyses? Maybe the defense challenges the integrity of the forensic swab, so the test needs to be recreated or confirmed. Perhaps, to bolster its case, the government now wants to pull data from the car's computer system to show the vehicle's speed at the time of the accident or that the breaks were never applied. All of this requires that the car, as evidence, was preserved and handled carefully to ensure it remained unchanged and uncompromised. It is also foreseeable that, in some situations, the car itself might be introduced as evidence or that some form of demonstration might be

---

215. A "trap" is a colloquial term for a hidden compartment built into a vehicle, which can be quite sophisticated and may require a specific procedure to open. *See* Brendan Koerner, *Alfred Anaya Put Secret Compartments in Cars. So the DEA Put Him in Prison*, WIRED (Mar. 19, 2013, 6:30 AM), https://www.wired.com/2013/03/alfred-anaya/ [https://perma.cc/QQ26-F8ET].

216. For the sake of this argument, assume that the police did not or were not authorized to search the entire car upon seizure, through either an accepted warrant exception or as an inventory search. However, thinking about how these accepted searches — beyond the scope of the original probable cause — might translate to a digital search is an interesting exercise that could be explored further.

given to the jury. Perhaps the government wants to show the jury the intricate process required to open the trap, such as setting the temperature to a specific setting while applying the break and lowering the passenger window. All of these considerations weigh in favor of retention, suggesting that it is reasonable and that the physical evidence seized need not — and should not — be subdivided.

2. Evidence Found in a Couch Cushion

Now suppose that law enforcement has been investigating a narcotics operation and believes it has identified the location where the drugs were being produced and distributed. The police prepare an affidavit and obtain a warrant based on the articulated probable cause. They search the suspected location and recover a couch cushion that is stuffed with bags of marijuana and that contains traces of a white powder that might be cocaine. The police seize this cushion and plan to conduct testing on the substance with the hope of introducing it as evidence at trial.

Now suppose that, some months later, the defendant's neighbor contacts the lead investigator and tells him that the defendant had raped her in his apartment. Because some time had passed, investigators cannot find any physical evidence to corroborate the victim's claims, so the case is essentially the victim's word against the defendant's, who claims that the victim has never been inside his apartment and that they have never had any type of sexual encounter. However, because the victim has several prior arrests, the prosecutor is concerned that the jury might not find her credible, meaning the case would not be proven beyond a reasonable doubt. Nonetheless, the prosecutor thinks there might be enough probable cause to obtain a warrant to examine the alleged crime scene. When officers execute the warrant, they find that the apartment has been entirely cleared out since the first warrant had been executed. Investigators then remember, however, that the couch cushion is still being held as evidence for the drug case. They get a warrant from a judge to swab the cushion, and subsequently find that it contains a mix of the defendant's and the victim's DNA — completely rebutting the defendant's story and greatly enhancing the victim's credibility. Were the retention, searches, and separate convictions unreasonable and violative of the Fourth Amendment? Should the government have somehow attempted to separate the substance from the cushion itself so the latter could be returned? Or is the evidence inextricably linked with the medium, thereby necessitating retention of what is arguably

not relevant for the sake of preserving the integrity of the forensic evidence?

3. A Bloody Sweatshirt

Consider a third hypothetical. The police are investigating a violent altercation, after which one of the participants succumbed to his injuries. They recover the victim's bloody sweatshirt, which, in addition to the victim's own blood, is suspected of containing blood or other trace evidence belonging to the other assailant. Forensic analysis identifies the perpetrator, and that individual is prosecuted for assault and homicide. Based on their interviews with the victim's associates — and entirely separate from any forensic analysis of the sweatshirt — authorities eventually suspect the victim was part of a domestic terrorism group. The police get a warrant to reexamine the sweatshirt,[217] this time looking to test it for any traces of explosives. The results come back positive for bomb-making materials, providing the probable cause for another warrant for the victim's residence. That search reveals a trove of damning evidence that also implicates the victim's roommate. Should the sweatshirt evidence, and its fruits, not be admissible for both the prosecution against the assailant and against the roommate? Does it matter that there would not have been probable cause for the apartment search, which led to the roommate's prosecution, had the government not retained the sweatshirt and later used it for a purpose other than the one for which authorities originally possessed it? Should the police have cut out the relevant bloodstain so that the rest of the sweatshirt could be returned to the victim's family? Would even the blood itself contain too much non-responsive information beyond the relevant details authorities needed?[218]

---

217. For excellent examples of how the government is regularly permitted to reexamine, *without a new warrant,* what has been lawfully seized, see Goldfoot, *supra* note 150, at 152 (citing cases involving clothing, cars, carpet fibers, purses, paper, videotapes, and even the defendant's hands). However, to fit the *Ganias* fact pattern, this analogy will assume that a warrant was obtained even though one might not be necessary.

218. In his article, Josh Goldfoot rightly suggests that the seizure of blood itself is an appropriate comparison to how digital evidence should be treated, as would be an examination of someone's clothing. *See id.* at 150 ("Blood is a good example of how courts treat physical evidence as objects, rather than containers of information. Like computer storage media, blood contains intermingled information, some irrelevant to an investigation. Examining a man's blood forensically can reveal whose blood it was, what he had been eating, what drugs or medicines he took, and, perhaps, whether he is sick. Yet, once officers lawfully seize blood, they may examine it without obtaining a warrant."); *id.* ("Every object has the potential to disclose facts

B. No Fourth Amendment Rights Were Actually Violated in *Ganias*

Despite the complexities raised by *Ganias*, no Fourth Amendment rights were actually violated. In making its finding of good faith, the court found that the agents had acted reasonably.[219] Under both the case law and the subsequently enacted Federal Rule of Criminal Procedure 41(e)(2)(B), imaging and later off-site review is permitted and is subject to review for *reasonableness*.[220] If the court found the agents acted reasonably and, thus, used the good-faith exception to avoid suppression of the evidence — assuming, *arguendo*, that a Fourth Amendment violation occurred — why is the agents' very same conduct not reasonable under a Fourth Amendment balancing? The court's same analysis should justify the retention and subsequent search. The agents sought and obtained a warrant for a distinct investigation using particularized facts — not once, but twice. In the course of its investigation, the government acted upon increased knowledge and new facts — as expected and desired in a search for the truth. Investigations regularly take twists or unexpected turns, and a search warrant or wiretap order can be supplemented or amended.[221] Here, warrants were obtained prior to each search based

---

about people who owned it, kept it, touched it, used it, moved it, or were just near it. Suppose a store clerk reports that the man who robbed her wore blue jeans stained with battery acid, and police obtain a warrant that allows them to seize a single thing: the blue jeans. That one item reveals information that is irrelevant to the investigation, and is also perhaps quite private. Forget the possibility that anything is in the pockets. The blue jeans tell us the man's waist size and let us guess if he is overweight or not. The brand tells us that he shops at Wal-Mart. Grease near the cuffs suggests he has ridden a bicycle. The smell suggests he has been around tobacco smoke. A worn right pocket suggests he favors that hand.").

219. *See* United States v. Ganias, 824 F.3d 199, 225 (2d Cir. 2016) (en banc) ("Finally, the record here is clear that the agents acted reasonably throughout the investigation. They sought authorization in 2003 to seize the hard drives and search them off-site; they minimized the disruption to Ganias's business by taking full forensic mirrors; they searched the mirrors only to the extent authorized by, first, the 2003 warrant, and then the warrant issued in 2006; they were never alerted that Ganias sought the return of the mirrors; and they alerted the magistrate judge to these pertinent facts in applying for the second warrant. In short, the agents acted reasonably in relying on the 2006 warrant to search for evidence of Ganias's tax evasion.").

220. *See supra* text accompanying notes 103–19.

221. *See, e.g.*, United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("Having found the rental agreement [for a storage locker during a lawful search of the defendant's home], the agents did not proceed lawlessly to search the locker; they presented their evidence to a magistrate who justifiably found probable cause to believe that a search of the locker would uncover evidence of drug trafficking."); United States v. Tortorello, 480 F.2d 764, 781–83 (2d Cir. 1973) (noting that nothing

on probable cause independent from the results of the search.[222] Where independent probable cause supports a new warrant, agents should be allowed to look where they could not before. If the agents' conduct was so reasonable that suppression was not warranted, how could that very same reasonable conduct not satisfy the reasonableness requirement of the Fourth Amendment?

Warrants protect privacy through the Fourth Amendment requirement that they issue only "upon probable cause."[223] This ensures that searches are conducted in a manner that minimizes needless intrusions on privacy. Here, two separate judicial authorizations found the invasion to be warranted. Law enforcement, in doing its job, is going to impose on people's privacy — rummaging through homes,[224] cars,[225] bags,[226] safe deposit boxes,[227] or even a person's body.[228] Warrants, or the application of one of the

---

requires the issuing judge to announce formally in open court that he noticed the interception of evidence not covered by the original order and that it is enough if notification of the interception of evidence not authorized by the original order is clearly provided in the renewal/amendment application papers); United States v. Gray, 78 F. Supp. 2d 524, 526–28 (E.D. Va. 1999) (describing how, during the execution of a warrant to search a computer for evidence of computer hacking, agents discovered child pornography and obtained a second warrant authorizing a search of defendant's computer files for child pornography).

222. For discussions of whether the plain-view exception to the warrant requirement should extend to searches of digital information, see, e.g., Michael Mestitz, Note, *Unpacking Digital Containers: Extending Riley's Reasoning to Digital Files and Subfolders*, 69 STAN. L. REV. 321 (2017); Andrew Vahid Moshirnia, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J. L. & TECH. 609 (2010); James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).

223. U.S. CONST. amend. IV.

224. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 246 (1983); Michigan v. Summers, 452 U.S. 692, 703 (1981); McDonald v. United States, 335 U.S. 451, 456 (1948).

225. *See, e.g.*, *Gates*, 462 U.S. at 246; Carroll v. United States, 267 U.S. 132, 147 (1925).

226. *See, e.g.*, Bond v. United States, 529 U.S. 334, 336 (2000); Robbins v. California, 453 U.S. 420, 428 (1981).

227. *See, e.g.*, United States v. Dunloy, 584 F.2d 6, 10–11 (2d Cir. 1978); United States v. Scolnick, 392 F.2d 320, 326 (3d Cir. 1968); United States v. Howell, 240 F.2d 149, 156 (3d Cir. 1956).

228. *See, e.g.*, Birchfield v. North Dakota, 136 S. Ct. 2160, 2184 (2016) (finding that the Fourth Amendment permits warrantless breath tests incident to arrests for drunk driving but that blood tests are significantly more intrusive and, thus, require either a warrant or some showing of exigent circumstances); Maryland v. King, 569 U.S. 435, 465 (2013) (permitting warrantless collection of a DNA sample as a negligible intrusion by rubbing a swab on the inside of a person's cheek); Cupp v. Murphy, 412 U.S. 291, 296 (1973) (upholding scraping underneath a suspect's fingernails to find evidence of a crime as a "very limited intrusion"); Schmerber v. California, 384 U.S.

enumerated exceptions, work to ensure that such encroachments are necessary.[229] In a recent and unrelated case dealing with modern technology, the Supreme Court observed that searches of digital devices raise new issues of scope given the amount and variety of data they can hold.[230] Here, however, there were warrants to search the computer because of *particular* and *articulated* wrongdoing stored thereon, which rendered the privacy incursion permissible. The Supreme Court in *Riley* did not find that the information stored within a cell phone was categorically immune from search; rather, the Court articulated that "[o]ur answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple — get a warrant."[231] *Ganias* deals with that latter situation, as the agents did get a warrant. Yet, there is no contention in *Riley* that a phone or a similar digital device could not be searched *after* a warrant has been obtained — or that there is then a ticking clock for its review.

Thus, having obtained a warrant and having searched Ganias's hard drives, the government could not have violated Ganias's expectations of privacy.[232] Once the devices were seized — or, rather, imaged — Ganias could have had no expectation that the government would not look through those materials.[233] He also would not have

---

757, 770 (1966) ("Search warrants are ordinarily required for searches of dwellings, and, absent an emergency, no less could be required where intrusions into the human body are concerned."); Sec. & Law Enf't Emps., Dist. Council 82, Am. Fed'n of State, Cty. & Mun. Emps., AFL-CIO v. Carey, 737 F.2d 187, 208 (2d Cir. 1984) (finding that a search warrant based on probable cause must be obtained before conducting a visual body-cavity search).

229. The warrant requirement has been described by the Supreme Court as "[t]he bulwark of Fourth Amendment protection," see Franks v. Delaware, 438 U.S. 154, 164 (1978), and there is no reason to believe that it cannot continue to serve in that role, whether the object to be searched is a digital device or a home.

230. *See* Riley v. California, 134 S. Ct. 2473, 2489–90 (2014).

231. *Id.* at 2495.

232. An "expectation of privacy" has been a bedrock principle of Fourth Amendment jurisprudence since Justice Harlan first enunciated the idea fifty years ago. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

233. *See, e.g.*, State v. Munro, 124 P.3d 1221, 1225 (Or. 2005) ("Here, the warrant lawfully authorized the seizure of the videotape and the invasion of defendant's privacy interest in its contents. Once the police seized the videotape under the authority of the warrant, any privacy interest that defendant had in the content of the videotape was destroyed by the authority of the warrant permitting the examination and exhibition of the contents of the videotape. Until such time as defendant regained lawful possession of the videotape, he had no remaining privacy interest in its contents that he could assert . . . . Once they lawfully had seized the videotape, nothing prevented the police from examining the contents of the videotape as often as they deemed necessary.").

been privy to what the government was looking at and when, irrespective of whether or not he was the target of the investigation. Thus, from his perspective, the agents could have discovered incriminating evidence immediately. His privacy interests in his property were found to have been outweighed by the showing of probable cause that there was specific evidence of wrongdoing. Therefore, if Ganias did not have any expectation of privacy, why would the seizure, searches, and retention be unreasonable under the Fourth Amendment? The protection he is given is that a sitting judge made sure that she believed there was probable cause before the search took place. This is the standard, whether it is a search of a digital document or of an intimate diary. Judges are the gatekeepers of privacy before law enforcement is allowed to infringe upon it, and the subsequent infringement is not *per se* unreasonable because it is an infringement. The agents did nothing wrong, and the court should not have been afraid to say affirmatively that there was no Fourth Amendment violation. Indeed, given that digital data were involved, it was all the more imperative for the court to understand the nuances of such data and articulate a clear and suitable standard.

In this case, the historical process for guarding against unwarranted government intrusions was clearly followed. There was an authorized search, which amounts to a justified invasion of Ganias's private data. Fruitful results were uncovered for use in a criminal prosecution. Numerous and legitimate reasons called for the retention of that data for said prosecution. Separately, additional facts supported an additional warrant, a further — but still lawful — intrusion into Ganias's privacy. Once more, fruitful results were discovered and were then used in a criminal prosecution. The agents could not have been expected to subdivide the data or more narrowly shape their efforts than they did, and their reasonable efforts satisfy the Fourth Amendment and ultimately amounted to quality police work. Rather than sidestep the issue, the court should have just said as much.

Permitting the police to use the additional evidence gives them a valuable tool to prove their cases and stop criminal actors. It provides an extra mechanism to protect public safety, with no added risk to privacy; the police have already conducted the search pursuant to a valid warrant. Subsequently denying the use of powerful evidence legitimately uncovered during a lawful search serves no deterrent purpose, misunderstands the nature of digital storage media, and needlessly rewards the malevolent actors.

CONCLUSION

To guard against governmental abuses and general rummaging through persons, houses, papers, and effects, the Fourth Amendment prohibits the issuance of a warrant absent probable cause and a particularized description of the authorized search.[234] The Fourth Amendment also requires that all searches and seizures are reasonable.[235] Thus, a reasonable search can be accomplished by securing a warrant, based on probable cause and particularly describing the place to be searched and the thing to be seized.[236]

In *Ganias*, the government obtained a warrant meeting these requirements and reasonably seized evidence, pursuant to the accepted two-step process for electronically stored information. The 2003 warrant authorized the lawful seizure of not merely particular records or data but the hard drives themselves — or, alternatively, the creation of full mirror images of the drives.[237] The warrant permitted their removal from the search premises for subsequent forensic examination. It set no additional limits on the government's retention of the drives than it did on any of the other evidence it authorized the agents to seize.[238] The government then reasonably used the fruits of that warrant, limited in scope, for the investigation for which it had been issued.

The government subsequently set forth independent information in a new affidavit and obtained a second warrant, also based on probable cause and describing what would be searched and what it hoped to seize. That second search was also fruitful, resulting in an additional prosecution and conviction. Throughout this process, the protections of the Fourth Amendment were in place, and its requirements were met multiple times. The application of the Fourth Amendment should not be altered just because digital data is involved. If the technology is faced head on, it is clear that the government acted appropriately. As such, and given that digital data is only becoming more pervasive and more relevant in court cases, the Second Circuit should not have dodged the issue, offering extensive dicta but no guiding precedent. Overcomplicating the technology can

---

234. *See* U.S. CONST. amend. IV. As discussed above, particularity requires the warrant to (1) identify the offense for which there is probable cause; (2) describe the place or thing to be searched; and (3) specify the object(s) to be seized in connection with designated crimes. *See supra* text accompanying notes 79–89.

235. *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

236. *See* U.S. CONST. amend. IV.

237. *See* Search Warrant, *supra* note 33.

238. *See id.*

overcomplicate the result, but if the courts would look past the mere skeuomorphism of computers, it is clear how a coherent physical item seized pursuant to a search warrant should be treated. Lawfully possessed items should be retained throughout the pendency of the investigation and prosecution, and if some legitimate purpose latter arises — within whatever relevant statutes of limitation that may apply — then the courts should be free to authorize further searches so long as they can be supported by sufficient probable cause — the controlling constitutional safeguard since the founding.

APPENDIX: A BASIC EXPLANATION OF COMPUTER DATA STORAGE

Hard drives are a complex innovation, and, generally speaking, most people are not aware of the inner workings of their computers, let alone the storage medium itself. However, to explain it simply, computers operate using binary language, which means that everything is represented by either a 1 or a 0.[239] Each 1 or 0 is known as a "bit."[240] Groups of eight bits are known as "bytes" and are the smallest unit of memory in computer architecture, representing a single number, letter, or character.[241] Computers use standardized encoding to translate human-readable language into binary, and vice versa.[242] Thus, when any file is saved to a hard drive, the computer is actually writing sequences of 1s and 0s (representing magnetic charges) to the disk, which, together, constitute a file.[243]

Hard drives generally create and read data through electromagnetism.[244] Traditional hard drives consist of metal platters

---

239. *See* SAMMONS, *supra* note 121, at 15–16.

240. *Id.*

241. *Id.* To illustrate, an uppercase letter "A" is represented in binary as the byte 01000001, while a lowercase letter "a" is 01100001. The number "1" is represented as 00110001, and a question mark is actually 00111111.

242. *Id.* The American Standard Code for Information Interchange ("ASCII") is the encoding scheme for the English language. ASCII Tables are charts that show characters and their corresponding computer language representations—such as binary, decimal, and hexadecimal, which use the mathematical bases 2, 10, and 16, respectively. These charts are readily available online, as are websites that will translate from one language into another. *See, e.g.*, *ASCII Table*, RAPIDTABLES, https://www.rapidtables.com/code/text/ascii-table.html [https://perma.cc/4U22-A9Y9]; BINARY HEX CONVERTERS, www.binaryhexconverter.com [https://perma.cc/X6AS-SMV6]; *ASCII, Decimal, Hexadecimal, Octal, and Binary Conversion Table*, IBM, https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/com.ibm.aix.networkcomm/conversion_table.htm [https://perma.cc/8RRN-F9QM].

243. SAMMONS, *supra* note 121, at 15–16. Readers can see this operation in action for themselves by creating a simple text file. Using a plain text editor such as Notepad (not a more advanced word processor, such as Microsoft Word), type a short phrase or message. Then, count the number of characters (including spaces) and save and close the document. Now, right-click on the file and view its properties. The file's size on the hard drive, indicated by the number bytes, should be the same as the number of characters in the file. This is because each character is one byte. On your hard drive, that file is actually stored as the sequence of 1s and 0s (bits) that translate to the ASCII characters of the file (bytes). The total file size is the number of bytes that the file requires on the hard drive. Rather than view the files on the hard drive as the user sees them, forensic tools can look at the raw data, the actual 1s and 0s on the hard drive that constitute the file.

244. *Id.* at 19. The majority of today's computer hard drives are magnetic drives, so this Note limits its discussion to traditional drives and does not address the advent of solid-state hard drives ("SSDs"), which are more advanced and operate entirely differently.

that rapidly revolve around a rod known as a spindle.[245] As these physical disks spin, a movable arm with a special read/write head hovers over the platters, with a microscopic gap between them.[246] In "write mode," the arm will magnetize points on the platter, which, in "read mode," are read as 1s.[247] Likewise, non-magnetized areas are read as 0s.[248] In essence, hard drives are simply spinning disks that are either raised or not along concentric tracks, with the resulting "topography" read just as a record player "reads" the grooves of a record.[249]

Computers store information in defined areas on the hard disk called sectors, which are the smallest "buckets" for data.[250] Each sector can typically hold up to 512 bytes of data — but no more.[251] Thus, computers store data as clusters — groupings of multiple sectors — which are the smallest physical units that can be allocated for data.[252] If a file's size is larger than the computer's cluster storage capacity, the system will assign additional clusters as needed, even if the final one is not fully used.[253] Thus, a file may be allocated to two clusters, filling the first and partially filling the second. In the second cluster, however, only the minimum number of sectors are used, rounding up to the next full sector.[254] However, the entirely unused sectors in the cluster, though allocated to the file, are not written with any new data.[255]

Computer file systems[256] are responsible for keeping track of this data, identifying what space is free, what space has been used, and

---

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.*

249. *See* CASEY, *supra* note 205, at 447 ("Data are recorded on a platter in concentric circles (like the annual rings of a tree trunk) called *tracks*." (emphasis in original)).

250. *See* SAMMONS, *supra* note 121, at 25.

251. *Id.*

252. *Id.*

253. *Id.*

254. If the data from the file itself fills only part of a sector in a cluster, the remainder of that 512-byte sector is filled with zeros. In other words, only whole sectors can be written at a time.

255. This process can result in the recovery of data from so-called "slack space," which is discussed below. *See infra* text accompanying notes 266–69.

256. There are a number of different types of file systems. FAT, or File Allocation Table, was used on older systems and is still used today on flash drives or similar devices. NTFS, or New Technology File System, was introduced with Windows XP and is still used today. HSF+, or Hierarchical File System, is used in Apple products.

where exactly each file is located.[257] The file system categorizes all space on a hard drive as either allocated or unallocated.[258] The computer user, through the operating system (such as Windows or Mac OS), can only view active files in allocated space.[259] Anything in unallocated space (such as a file after it has been "deleted") is invisible to the operating system, though, on the hard drive itself, it is simply marked as "not in use" — which does not mean that the space is empty.[260]

Latent data refers to data that has been deleted or partially overwritten.[261] Essentially, when a user deletes a file, the computer eliminates the entry in its file system table — where used/unused clusters and their locations are recorded — making the file invisible to the computer user by ordinary means and the physical space where it resides available for use when the computer is saving future files.[262] However, until a given cluster is reused, the data itself remains untouched and can be recovered by forensic examiners.[263]

To complicate matters further, a single file is not necessarily stored in one place and may be scattered across various clusters on the hard drive platters.[264] This is why the file system not only tracks what areas of the hard drive have been used but also notes where a particular file is stored[265]; a single document or photo might be saved in contiguous clusters, or it could be fragmented and saved in a number of non-contiguous clusters.[266] Additionally, when data are

---

Though there are some nuances among the three, they all serve the same essential function. *See id.* at 23.

257. *Id.*

258. *Id.* at 24. In essence, the computer logs "this area is used, do not write here" or "this space is available, data can be stored here."

259. *Id.* at 22, 24.

260. *Id.*

261. *Id.* at 22.

262. *Id.* at 22–24. Most modern operating systems, irrespective of their differences, merely erase the "pointer" to the file so it no longer appears in directory listings. However, they do not erase the actual data. Sammons uses the analogy of a book index, which, like the file system, lists the information and its location. He explains, "Using the book analogy again, deleting a file would be akin to removing the entry from the book's index. Although our subject is no longer referenced in the index, the page and all its contents are still in the book, intact and untouched." *Id.* at 24.

263. *Id.* at 24 ("Deleted files will sit there until they're overwritten by more data . . . . With the massive amount of storage space available on today's hard drives, a file stands a good chance of never being overwritten.").

264. *Id.*

265. *Id.*

266. *Id.* at 24–25. Some readers may have used the system tool "Disk Defragmenter" to analyze their hard drives and move disparate file pieces closer

written to a space on a hard drive that had previously housed a now-deleted file, it is possible that the new file will not use the entirety of the cluster.[267] If the prior file filled more sectors than the new file uses, the last few sectors of the cluster allocated to the new file may actually contain the data from the prior file — which will not be overwritten since the file system marks the whole cluster as in use.[268] In computer forensics lingo, this is known as data in slack space, the difference between the space that is assigned and the space that is actually filled.[269] For both deleted files that have not yet been overwritten at all or for remnants of files that have only been partially overwritten and persist in slack space, forensic examiners can use standard forensic tools to recover them.[270]

Examiners can use a process called "carving" to extract data from undifferentiated blocks of raw data in unallocated space.[271] Examiners can search through the sequences of bits and bytes that make up files and look for file headers and footers, which identify the files and mark the beginnings and ends of the data.[272] Users are unlikely to contemplate the amount of revealing information that is unintentionally created or that is tracked by hidden system files, such as data in a hibernation file,[273] swap file,[274] registry or system logs,[275]

---

together so the data can be read more quickly by the actuator arm moving over the disks. Because it is a mechanical process, when pieces of a file are stored in multiple locations, it takes longer for the arm head to move to and read each cluster to reassemble the file when a user wants to open it. Defragmenting moves the pieces closer together so the file can be made available more quickly.

267. *Id.* at 25.

268. *Id.* at 25–29.

269. *Id.* at 25, 28.

270. *Id.* at 26–27.

271. *See* CASEY, *supra* note 205, at 445–46. This technique can be conducted manually or with a tool and involves identifying known file signatures within the morass of 1s and 0s. Relevant fragments are carved out, just as a sculpture is "carved out" of a solid stone.

272. *See id.*; SAMMONS, *supra* note 121, at 17, 66.

273. When a user places his or her machine into hibernation, all of the temporary and volatile data in Random-Access Memory ("RAM") is written to the hard drive as the file "hiberfil.sys" so it can be retained while the device is completely powered down. The effects of this do not simply vanish when the user starts the machine again, as data written to a hard drive are more persistent, preserving the active session far longer than the user would presume and making the data more likely to be recovered by investigators. *See* CASEY, *supra* note 205, at 385, 497.

274. Swap files enable a computer to run more processes, supplementing its physical RAM by temporarily storing information that is not being used on the hard drive itself, "swapping" or "paging" data into and out of RAM as required. *See id.* at 384, 456, 496–97.

restore points,[276] or a thumbnail cache.[277] Even lack of data could be telling, as specific patterns on the bit-level might suggest an attempt at concealment[278] and signal to investigators to look for other signs of data concealment.[279] All of this information is contained in the raw sequence of 1s and 0s — not the visible files — and can be tremendously useful in furthering an investigation.

With respect to the files in allocated space that the user can see, the file system maintains various metadata about the data.[280] It logs the dates and times that each file or folder was last modified, accessed, and created — collectively known as "MAC times" — as well as information about the author or user. Similarly, the web browsers a user installs to access the Internet can store a great deal of detailed information about the user's activity and habits, tracking information about recently visited websites, downloads, or search terms entered.[281] As with latent data, metadata regarding active data could

---

275. On Windows computers, the registry serves as a central database of the computer's settings and configurations. It can reveal information about programs that were installed, terms searched, recently opened documents or program, password information, user profiles and their permission settings, attached media and devices, and many other details. *See id.* at 535–38; SAMMONS, *supra* note 121, at 68.

276. Restore points "are snapshots of key system settings and configuration at a specific moment in time" that can be created automatically upon certain triggering events (such as before installing new software), at regularly scheduled intervals, or manually by the user. SAMMONS, *supra* note 121, at 79. Microsoft hides them from the user and includes metadata about when they were taken. *See id.* As a result, the user might not have thought to delete them, so they can reveal valuable information that does not exist on the live system and can show exactly when that data existed on the machine.

277. Windows automatically creates thumbnails, small versions of larger photographs, to make it easier to browse the pictures on a computer. Because these files remain after the original images have been deleted—and users might not be aware that they even exist—thumbnails can serve as evidence to prove that the pictures existed at some point on the system. *See id.* at 78.

278. The appearance of "normal" bits—what the hard drive would look like after everyday use—is somewhat random and inconsistent. If a distinct pattern appears in a particular area of data, it could indicate that the user made a concerted effort to permanently overwrite what had been there with random new data. A forensic examination could reveal telltale signs of the presence or use of data-wiping tools that may have been installed in an attempt to make data unrecoverable. This alone could serve as valuable evidence, or it could serve as a clue for the analyst for how to proceed to try to recover evidence. *See id.* at 96.

279. *See id.* at 80.

280. *See id.* at 75–76.

281. *See* CASEY, *supra* note 205, at 538–42 ("Accessing the Internet leaves a wide variety of information on a computer including Web sites, contents viewed, and newsgroups accessed . . . . [S]ome Windows systems maintain a log of when the modem was used . . . . When an individual first views a Web page, the browser caches

be lost or altered were files to be removed by a means other than careful forensic imaging. Such loss of evidence could mean the difference between a case going unsolved and a criminal defendant being brought to justice.

---

the page and associated elements . . . . The number of times that a given page was visited is recorded in some Web browser history databases.").