1-1-2020

The Fourth Amendment Inventory as a Check on Digital Searches

Laurent Sacharoff
University of Denver, lsacharoff@law.du.edu

Recommended Citation
The Fourth Amendment Inventory as a Check on Digital Searches, 105 Iowa L. Rev. 1643 (2020).

The Fourth Amendment Inventory as a Check on Digital Searches

Publication Statement

Copyright held by the author. User is responsible for all copyright compliance.

Originally published as The Fourth Amendment Inventory as a Check on Digital Searches, 105 Iowa L. Rev. 1643 (2020).

The Fourth Amendment Inventory as a Check on Digital Searches

Laurent Sacharoff[*]

ABSTRACT: Police and federal agents generally must obtain a warrant to search the tens of thousands of devices they seize each year. But once they have a warrant, courts afford these officers broad leeway to search the entire device, every file and folder, all metadata and deleted data, even if in search of only one incriminating file. Courts avow great reverence for the privacy of personal information under the Fourth Amendment but then claim there is no way to limit where an officer might find the target files or know where the suspect may have hidden them.

These courts have a point. How can an officer know where she will find evidence of, say, drug trafficking until she has opened and at least skimmed most files? When scholars and courts try to protect privacy with ex ante *limits, they engage in laudable efforts possibly doomed to fail. Moreover, these* ex ante *solutions presume that the Fourth Amendment protects privacy-as-secrecy only—the right not to have the files viewed at all. True, secrecy over papers is a basic right, but the Fourth Amendment protects far more; it protects the right "to be secure" in one's "papers."*

This Article is the first to propose an entirely new method to protect Fourth Amendment security in papers rooted in the ancient inventory and return requirements for executing warrants. In the physical world, officers must prepare an inventory of each thing they seize pursuant to a warrant. I argue we should apply this inventory requirement to electronic information and, in particular, to each file an officer views.

Providing the inventory will further a person's right to be secure in her papers for several reasons. She will know which files officers viewed, and which they did not. She will be able to compare those files with the authorization of the warrant. Courts and individuals will, for the first time, have the ability to supervise officers' searches and seek remedies for searches that go beyond the scope of the warrant. Finally, the threat of remedy will deter over-broad searches. This ex post *protection will effect* ex ante *limits.*

---

[*] Professor of Law, University of Arkansas School of Law, Fayetteville; J.D., Columbia Law School; B.A., Princeton University. The author thanks Ric Simmons, Steven Morrison, Orin Kerr, Jordan Woods, Anna Roberts, Lauryn Gouldin, Ellen S. Podgor, Alan M. Trammell, as well as the participants of the 2018 Northeast Privacy Scholars Workshop. He also thanks Hannah Butler for excellent research assistance.

I. INTRODUCTION

Electronic devices store gigabytes of information about our lives. It has become commonplace to observe that the framers of the Fourth Amendment could not have foreseen smartphones or computers collecting all our messages, our documents, our finances, and our family photos.[1] In applying the Fourth Amendment to electronic devices, we can therefore learn little from that founding generation or the problems that led it to insist upon a search and seizure provision in the Bill of Rights.[2]

But our use of electronic devices reflects the framers' experiences as much as it deviates from them. The framers, and many of their English heroes, were highly educated people who possessed nearly as wide an assortment of papers as a contemporary smartphone user: personal letters, financial documents, deeds, wills, bank bills and accounts, books, newspapers, drawings, poems, architectural plans, diaries, calendars, scientific studies and notes, and probably much more.[3] Their diaries often recorded their daily or even hourly location, activities, and companions.[4] They likewise had strong reactions to the problem of government searches of these papers for incriminating evidence in criminal cases.

How did the founding-era English and American elite, courts, and legislatures react to the search of papers in a criminal case? They prohibited it.[5] Scholars have recently coalesced around an astounding premise: The framers, anyway, intended the Fourth Amendment to ban searches and seizures of papers for criminal cases. In fact, the common law practice at the time likewise barred such seizures.[6] When we consider why, we face arguments that closely parallel those today concerning searches of electronic devices.

---

1. Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1211 (2014) ("When the Framers wrote the Fourth Amendment and later carved out an exception for border searches, they did not foresee the smartphone, the laptop, sexting, or cloud storage."). Kugler does note, nevertheless, the framers' protectiveness of papers. *Id.*; *see also* Richard A. Posner, *What Is Obviously Wrong With the Federal Judiciary, Yet Eminently Curable: Part II*, 19 GREEN BAG 2D 257, 258 (2016) ("It thus is silly to ask whether . . . the Fourth Amendment forbids electronic surveillance . . . . [Its] authors and ratifiers had no opinion on electronic surveillance . . . ."). *But see* William Baude & Stephen E. Sachs, *Originalism's Bite*, 20 GREEN BAG 2D 103, 107 (2016) (criticizing Posner for thinking on too particular a level of generality).

2. *Cf.* Riley v. California, 573 U.S. 373, 385–86 (2014) (noting that the framers gave no guidance on how to balance the privacy interests of an arrestee carrying a smartphone against law enforcement interests, because smartphones allow a person to carry all her papers with her).

3. Entick v. Carrington, 19 Howell's St. Tr. 1029, 1065 (CP 1765) ("Accordingly, all was taken, and Mr. Wilkes's private pocket-book filled up the mouth of the sack.").

4. *E.g.*, JOHN WILKES, THE DIARIES OF JOHN WILKES 1770–1797, at 29 (Robin Eagles ed., 2014) ("[L]eft Marlborough at ten, came to the Devizes, the Bear, Maltby's, at 12, reach[e]d Bath at two, dined at the Bear, Phillot's, lodged at Mrs Harford's the last house on the South Parade, towards the river. Miss Wilkes continued in Prince's Court." (second alteration in original)).

5. *Entick*, 19 Howell's St. Tr. at 1073 (even for "murder, rape, robbery, and housebreaking . . . our law has provided no papersearch [sic] in these cases to help forward the conviction.").

6. Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 568 (2017) ("[C]onsistent with common law, judges did not have the authority to issue search warrants to seize papers as evidence of criminal activity."); Laura K. Donohue, *The Original*

First, papers enjoy the greatest privacy, more than ordinary property, which already enjoyed sacred protection under English common law.[7] Second, even if it were permissible to seize those particular documents that were incriminating, there would be no way officers could find those documents without seizing and searching through 100 innocent papers for every guilty one.[8]

But these precedential English cases reflected other core principles: procedural safeguards. The searches were apparently deemed unlawful in part because no one created an inventory of the papers taken or supervised the search to ensure the officials did not take valuable papers, such as bank bills, and the officers did not return the warrant and seized items to the court for review.[9] These often-neglected ancillary lessons from these early cases provide important clues to solutions today.

We have strayed far from these lessons, however. Today, the Fourth Amendment permits law enforcement to search and seize papers in criminal investigations. When it comes to digital devices, moreover, magistrate judges now routinely issue warrants authorizing police or federal agents to seize suspects' digital devices and search every nook and cranny.[10] If the agents seek even one incriminating document, they often enjoy the power to open every file and folder, and review metadata, location data, and deleted data.[11]

Fourth Amendment, 83 U. CHI. L. REV. 1181, 1311 (2016) ("[T]he government could neither rummage around in one's personal documents nor comb through one's business records to uncover evidence of criminal behavior."); Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 52 (2013) ("The one Founding-era attempt to authorize seizing papers by statute was condemned as contrary to common law and natural right and never passed into law."); Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 921 (1985) ("Read in light of its historical background, the [F]ourth [A]mendment's search and seizure clause condemns the inspection of innocent private papers by government officials in search of a document that by itself may be unprotected."). *But see* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 727, 727 n.512 (1999) (arguing that the "claim that the Framers would have viewed any seizure of papers as compelled self-incrimination" is "fanciful at best").

7. *Entick*, 19 Howell's St. Tr. at 1066 ("Papers are the owner's goods and chattels: they are his dearest property."); *see* Boyd v. United States, 116 U.S. 616, 622–23 (1886); *see also* Gouled v. United States, 255 U.S. 298, 309 (1921) ("[Search warrants] may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding . . . .").

8. *E.g.*, Schnapper, *supra* note 6, at 917–18.

9. *Entick*, 19 Howell's St. Tr. at 1064–65. The court emphasizes the absence of these protections, but their precise significance in relation to the ultimate holding is unclear. *Id.*

10. United States v. Evers, 669 F.3d 645, 649–50 (6th Cir. 2012); United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders."). *See generally* Adam M. Gershowitz, *The Post-*Riley *Search Warrant: Search Protocols and Particularity in Cell Phones Searches*, 69 VAND. L. REV. 585 (2016) (noting and critiquing lack of *ex ante* limits).

11. United States v. Krupa, 658 F.3d 1174, 1178 (9th Cir. 2011) (approving search of 15 computers based on one image); United States v. Brobst, 558 F.3d 982, 988 (9th Cir. 2009) (authorizing "the search and seizure of 'photographs . . . computers, compact disks, floppy disks, hard drives, memory cards, printers, and other portable digital devices, DVDs, and video tapes'" based on a witness' observation of one illicit photograph in defendant's home).

True, warrants must list the places to be searched, and the items to be seized, with "particularity." But most magistrates meet this particularity requirement by listing the electronic device as the thing to be seized (and the place to be searched).[12] They need not list any particular files on the device to be searched beyond broad categories, such as "financial documents evidencing fraud." And more important, the warrant need not limit *where* on the device law enforcement may search.[13]

Courts have largely thrown up their hands when it comes to imposing limits on law enforcement searches of digital devices. These courts ask, in effect, "how can a warrant specify in advance where agents may look for incriminating files until they have actually looked?"[14] After all, agents authorized by warrant to search a home for drugs may search anywhere drugs may be found, which is anywhere—living rooms, bedroom, closets, basements, dressers, drawers, jewelry boxes, and even toilet tanks.[15]

How do we escape this morass?

We could return to an originalist view and simply prohibit the criminal authorities from seizing and searching electronic devices entirely. But as discussed below, that course goes too far.[16] We can ameliorate the problem by taking the particularity requirement seriously to sharpen limits to the search both *ex ante* and *ex post*.

First, we can still try to impose meaningful *ex ante* limits on where officers may search, limits made more possible by recent technological developments.[17] But these *ex ante* limits will not impose significant protections;[18] moreover, they treat the Fourth Amendment as synonymous with privacy-as-secrecy only. Limiting which files law enforcement may open and view primarily protects the secrecy of the data, but this narrow conception of privacy harms misses many other interests individuals have in their data such as understanding how it is being used, control over that use, and the return and destruction of the data when appropriate.

Therefore, second, in a major contribution, this Article proposes we apply the inventory requirement implicit in the Warrant Clause to electronic data and individual files.[19] Currently, officers who execute warrants must

12. *E.g.*, FED. R. CRIM. P. 41(e)(2)(B); State v. Goynes, 927 N.W.2d 346, 351 (Neb. 2019); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 6 (2015).

13. United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013).

14. *E.g.*, *id.* ("The government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 575 (2005).

15. Guishard v. United States, 669 A.2d 1306, 1310 (D.C. 1995), *abrogated by* Robinson v. United States, 100 A.3d 95 (D.C. 2014) (during a search pursuant to a warrant, a "ziplock bag containing five smaller bags of cocaine was found inside the toilet tank in the bathroom").

16. *See infra* Part VI.

17. *See infra* Part III.

18. *See infra* Part III.

19. *See* Berger v. New York, 388 U.S. 41, 57 (1967).

prepare an inventory of all the physical items they seize, and return that inventory to the court and provide it to the individual.[20] Unfortunately, when applying this requirement to the electronic world, courts have required agents simply inventory the device seized, not individual files viewed or copied.[21] An inventory would simply say, for example, "one iPhone 6, serial number ###."[22] Federal Rule of Criminal Procedure 41 seems to endorse this view.[23] I show below why the inventory should instead require a list of each file opened, viewed or copied.

This very new—and yet very old—Fourth Amendment inventory proposal protects what lies at the heart of that provision, protecting the right to be "secure" in one's "papers." To be secure means more than privacy-as-secrecy. It includes, or I argue should include, the power of an individual to understand which information has been exposed, and which has remained secret.[24] Under my proposal, a person will, for the first time, know precisely which files and folders agents have viewed or copied, affording her greater security through transparency.

To be secure also includes a person's right to compare the scope of the search with the lawful authorization contained in the warrant, to decide for herself whether the agents obeyed the law.[25] The prominent English cases leading to the Fourth Amendment themselves hinted this inventory requirement for ordinary property should apply to individual papers for this reason.[26] This right to compare leads to the power of remedy; a person can sue for an overbroad search only if she knows where the agents actually did search. Agents, meanwhile, aware that the scope of their searches will, for the first time, be transparent to suspects and the court alike, will take greater steps to curtail the scope of those searches. The *ex post* remedy will effect an *ex ante* limit.

In addition to an inventory, I also propose that individuals will have the right to recover their electronic data—except for contraband—similarly furthering their security and property rights. The government will have to destroy its copies to the extent not required for investigation or trial. This follows from the analogy to ordinary property—when the government hands back a person's property, it obviously can no longer retain it.

---

20. *E.g.*, FED. R. CRIM. P. 41(f)(1)(B). Part IV below discusses whether the Warrant Clause requires an inventory or has simply been assumed throughout history to.

21. *E.g.*, United States v. Schesso, 730 F.3d 1040, 1050 n.8 (9th Cir. 2013) (citing FED. R. CRIM. P. 41(f)(1)(B)).

22. *E.g.*, Inventory of Items Seized, United States v. Hyatt's Suboxone Clinic, No. 5:18-mj-00047 (W.D. Va. Aug. 20, 2018) ("Acer laptop"); *see infra* note 116.

23. *See* FED. R. CRIM. P. 41. Despite the rule language, the committee notes make clear that the rule remains neutral on the question. *Id.*

24. Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1906 (2013) ("Effective privacy regulation must render both public and private systems of surveillance meaningfully transparent and accountable.").

25. *See* Groh v. Ramirez, 540 U.S. 551, 558–59 (2004).

26. *See* Entick v. Carrington, 19 Howell's St. Tr. 1029, 1067 (CP 1765).

The requirement that the government destroy its copies of most of the data *soon* brings even further security to the individual. The data are less likely to be hacked or leaked. The person can rest easier simply knowing the government has not retained her entire digital life. But most important, under my proposal, agents will not be able to retain gigabytes of a person's data for later data mining, over a period of years, for new crimes, under new theories—as happened recently in the *United States v. Wey* case, detailed below.

The inventory requirement will impose little to no burden on government agents because the forensic software they use to search the device can be configured to generate a report listing all the files opened or copied. In fact, forensic software used by law enforcement around the country will begin to evolve to take account of these new requirements and limits, helping agents to stay within reasonable bounds as developed by case law and commonsense.

My proposal asks that we amend federal and state statutes to require officers to make and supply an inventory of individual electronic files opened in order to safeguard the Fourth Amendment values of privacy and security. My proposal also argues that the Fourth Amendment itself requires such inventories. After all, inventories (whether written or part of the physical return) formed a critical enforcement mechanism of a warrant's particularity requirement—both at the founding and today. That is, the particularity requirement insists that officers seize only items a magistrate listed in advance. The inventory and return allow the magistrate to determine whether the officer observed the limits or, instead, seized items that did not match the items, or type of items, listed in the warrant.[27] The inventory also serves as evidence in any subsequent lawsuit over whether the property was lawfully seized.

Magistrates thus perform a matching function upon the return to ensure the items seized are those described in the initial warrant. This matching function links the inventory and return requirement to the express particularity language in the Warrant Clause so as to make the inventory not only a historical complement to the warrant, but also a constitutional element of it. To the founding era, the term "warrant" included as part of its definition an inventory, either written or in the form of a return of the things seized—a uniform practice reflected in founding era justice of the peace manuals governing warrants, contemporary statutes, and case law.[28] Put another way, the founding era would have found the execution of a warrant to seize items to be an "unreasonable" seizure without such an accounting.

But note: I do not argue as part of my proposal that a failure of law enforcement to prepare an inventory should trigger the exclusionary rule. Rather, the remedy for no inventory is simply for the court to require law enforcement to prepare one. Indeed, my main point is that the inventory itself facilitates the remedy: furthering security through transparency, facilitating a

27. United States v. Birrell, 269 F. Supp. 716, 721 (S.D.N.Y. 1967) (inferring the purpose of the inventory required under Rule 41).

28. *See infra* Section IV.C.1.

return to the suspect of unneeded files (and their destruction), and serving as evidence in any later litigation.

Now some courts, including the Supreme Court, have held in passing that an incomplete inventory does not violate the Fourth Amendment;[29] others have held that the Fourth Amendment does not require an inventory or return on the warrant at all,[30] or even require law enforcement to give property back to the individual that it has unlawfully seized or retained.[31] These cases were wrongly decided at the time and, in any event, almost entirely undermined by the Supreme Court's holding in *Manuel v. City of Joliet*.[32]

A note on scope: This Article focuses on devices. But law enforcement serves hundreds of thousands of subpoenas, warrants, and other orders each year on third-party providers such as Verizon or Facebook to produce emails, messages, location data, posts, photos, and other account information. In this arena too, law enforcement rarely if ever provides a person with an inventory of the information they obtained or viewed. My proposal should apply equally to this realm, at least when a warrant is required, and probably to subpoenas as well.

Part II examines the current broad searches courts too often endorse for electronic devices. Part III shows how technological developments—the sandbox model of programming—provide courts with a new tool to limit searches to those folders or apps likely to contain the incriminating evidence. It refutes the too-commonly asserted complaint that ordinary suspects can hide data anywhere on the device. With mobile devices, they cannot. Courts and scholars have largely ignored how this critical technological advance changes digital searches.

Part IV—the heart of this Article—presents an entirely novel proposal requiring agents to create an inventory of files viewed and copied.[33] This application of the inventory requirement to electronic files will further core Fourth Amendment values, both privacy and security.

Part V addresses potential objections, such as whether opening a file counts as a "seizure."

Part VI draws on founding era sources—case law, statutes, treatises, and practice—to show that the inventory and return requirements likely formed part of the original understanding of the Fourth Amendment. True, the framers also likely banned any searches and seizures of papers for evidence of a crime. But they also hinted that *were they* to allow such searches, they would have required officers to have created an inventory of the papers seized just as for other things.

---

29. Cady v. Dombrowski, 413 U.S. 433, 449–50 (1973).

30. *E.g.*, United States v. Dudek, 530 F.2d 684, 691 (6th Cir. 1976).

31. Denault v. Ahern, 857 F.3d 76, 84 (1st Cir. 2017) (collecting cases).

32. Manuel v. City of Joliet, 137 S. Ct. 911, 918–19 (2017); *see also infra* Section VI.D (giving further discussion on *Manuel v. City of Joliet*).

33. I use the term "file" as the thing to be seized and listed in the inventory, but for some data, a single file will not be the correct measure, as discussed in Part IV.

II. UNCOMMONLY BROAD SEARCHES

This Part illustrates the breathtaking scope of digital searches even once government agents have obtained a warrant. It first discusses a recent and prominent FBI search in *United States v. Wey*,[34] an insider trading case that illustrates almost all the drawbacks of the current regime. It next shows how courts fail to supply meaningful limits in issuing warrants or in reviewing searches after the fact at a suppression hearing. Agents who make bare showings of probable cause that a certain type of document appears on a device have free rein to search every file and folder for that one incriminating type of document. Finally, it shows why courts have imposed such lackluster limits—partly for understandable reasons flowing from the nature of a paper search, and partly based on courts' misunderstanding of the technology and forensic software.

A. UNITED STATES V. WEY

Benjamin Wey presents a modern-day character nearly as colorful as John Wilkes, the Englishman whose cases in the 1760s led to many of the Fourth Amendment's protections. Wey founded and ran a successful securities business specializing in "reverse mergers."[35] These allowed larger Chinese companies to merge with small, existing U.S. shell companies already traded in the United States, allowing the Chinese companies to secure a quicker foothold in U.S. markets than they might otherwise.[36]

But Wey also promoted and promotes himself as a journalist. He publishes (apparently)[37] and writes in TheBlot Magazine,[38] a financial and general interest blog aggregator covering numerous finance stories, including those that focus on himself and his self-proclaimed victories.

But as relevant to us, Wey suffered broad, exploratory searches and seizures of his papers (and electronic devices) in both his home and office —searches that a federal court later deemed indistinguishable from a "general search" in violation of the Fourth Amendment.[39] The FBI searches violated nearly every principle the Warrant Clause protects. In addition, they violated nearly every principle the English courts adduced in the 1760s for finding the searches then unlawful under fundamental common-law principles.

---

34. United States v. Wey, 256 F. Supp. 3d 355 (S.D.N.Y. 2017).

35. *Id.* at 359–60.

36. *Id.*

37. Pending libel litigation leaves open whether he does, in fact, publish the magazine. *See generally* Brummer v. Wey, 166 A.D.3d 475 (N.Y. App. Div. 2018) (remanding to determine this question).

38. *See generally* THEBLOT MAGAZINE, https://www.theblot.com [https://perma.cc/N7NJ-FU9W].

39. *Wey*, 256 F. Supp. 3d at 410 (suppressing everything seized because agents' search was "essentially indistinguishable from a general search" (quoting United States v. Shi Yan Liu, 239 F.3d 138, 141 (2d Cir. 2000))).

Before we summarize those principles, we may sketch the facts. The FBI was investigating Wey for securities fraud and disclosure violations.[40] It obtained a warrant to search his office and home.[41] The warrant did not list the crimes for which the FBI had probable cause, nor the type of papers it sought with particularity.[42]

At Wey's office, agents seized Wey's cellphone and 24 computers or other electronic devices.[43] They also copied or mirrored the cellphones of all the employees on the premises without first determining whether those devices contained relevant evidence.[44]

At Wey's apartment, 17 agents searched everywhere, including the children's bedrooms, and seized about 4000 hard documents, including soiled documents in garbage cans.[45] The Court noted that they seized numerous personal and sensitive documents, including medical information, x-rays of family members, Wey's living will and healthcare directives, family photos, and the children's school test scores.[46]

In addition, government agents seized or copied 25 electronic devices from the home, including the cellphone of Wey's wife, who was allegedly also a bookkeeper for the company.[47]

For two years after the search, federal agents kept the electronic data and continued to data mine files, terabytes of data, for new crimes not listed in the original warrant or affidavit, in addition to running new names, also not in the original affidavit, as search terms.[48]

The district court ultimately found that both the warrant and its execution violated the Fourth Amendment so gravely that the court suppressed all the evidence obtained, leading the government to dismiss the case.[49] Along the way, the court noted the numerous Fourth Amendment principles the FBI had violated—principles we will see almost precisely parallel those enunciated in the English cases from the 1760s.

We can divide these principles into three categories. First, the warrant itself failed to satisfy the particularity requirement of the Fourth Amendment.[50] Second, the officers executing the warrant exceeded its scope.[51] Third, for years afterwards the FBI retained and used the

40. *Id.* at 361.
41. *Id.* at 363–64.
42. *Id.* at 410. Rather, many of these details were in affidavits that were not incorporated into the warrant. *Id.* at 363–65.
43. *Id.* at 370.
44. *Id.*
45. *Id.* at 372.
46. *Id.* at 372–73.
47. *Id.* at 373.
48. *Id.* at 377–78.
49. *Id.* at 409.
50. *Id.* at 384.
51. *Id.* at 384–88, 398–99.

information.[52] For our purposes, especially with respect to my inventory proposal, the problems the court found wanting under this third category were:

- the agents kept the vast trove of information they obtained for years without any accounting, itemizing, or inventory;[53]
- the agents refused to return the information or devices for years until ordered to do so by a judge;[54] and
- the government agents engaged in a fishing expedition during this time, and data mined the data for evidence of new crimes not listed in the warrant or affidavit by searching documents previously determined not to be relevant.[55]

The court found the last-listed conduct particularly problematic. We may note that such subsequent rummaging through papers for new crimes is the very definition, for both the founding generation[56] and contemporary courts,[57] of the fishing expedition the Fourth Amendment (and likely Fifth Amendment)[58] sought to prevent.

We may be tempted to deem the searches in *Wey* outliers. But consider further that the FBI worked closely with Preet Bharara's U.S. Attorney's Office in the Southern District of New York, the premier office for investigating and prosecuting securities fraud cases. The government had spent months investigating and preparing the case before seeking the warrants, and a well-respected federal magistrate judge approved them. Agents prepared carefully for the searches themselves, with 20 agents reviewing an "operations order form" setting forth the search protocol.[59] Even though the district court detailed the warrant's flaws, the judge recognized that the lawyers and agents had not acted with malice; they had prepared carefully for an important and high-profile case.[60]

Rather than deeming the *Wey* searches as outliers, we can draw a different conclusion: The case instead illustrates the hazards that await any search and seizure that involves possibly incriminating material mixed with tremendous

52. *Id.* at 405–08.

53. *Id.* at 405.

54. *Id.* at 373.

55. *Id.* at 377–78.

56. Dripps, *supra* note 6, at 70 ("It is a fishing for evidence . . . ." (quoting A LETTER FROM CANDOR, TO THE PUBLIC ADVERTISER 31 (J. Almon ed., 2d ed. 1764))).

57. United States v. Foster, 100 F.3d 846, 852 (10th Cir. 1996) (noting "a 'fishing expedition' for . . . additional crimes" violates purpose of particularity requirement); *see* United States v. Uzenski, 434 F.3d 690, 706 (4th Cir. 2006) (same).

58. United States v. Hubbell, 530 U.S. 27, 32, 34 n.8 (2000) (finding a Fifth Amendment violation that the district court had described "as 'the quintessential fishing expedition,'" and noting the roots of the Fifth Amendment lie, in part, to prevent wide exploration "to uncover uncharged offenses, without evidence from another source." (citations omitted)).

59. *Wey*, 256 F. Supp. 3d at 367.

60. *Id.* at 408.

volumes of innocent business, personal, or private information, all exacerbated by the storage capacity of electronic devices. As discussed below, at least some of these problems lie inherent in the entire enterprise of searches of papers —a conclusion the founding generation had already reached by the latter half of the 1700s.

B. SUMMARY OF EXISTING LIMITS

The Supreme Court has yet to address how warrants or their execution apply to digital evidence, but lower courts have imposed very few meaningful limits. First, the warrant must list the crime or crimes that gave rise to probable cause.[61] Second, the warrant must list the place to be searched. For this requirement, the warrant usually only needs to list electronic devices in general[62]—any device that might be found on the premises—rather than establishing probable cause to believe a particular device contains relevant evidence. Third, the warrant must list the "things" to be seized and link those "things" to the crimes, but the "things" can be described in broad categories.[63] For example, the warrant can seek all financial documents relating to income for the years 2010–2012 concerning an alleged tax fraud.

Agents often can meet the above requirements, and in the execution of the warrant, law enforcement ends up searching nearly every part of a device, with the right to open nearly every file. Courts almost uniformly allow agents to seize entire devices and take them back to the lab for comprehensive forensic review, rather than review them onsite as agents might with ordinary property.[64] Rule 41, which governs federal agents, expressly permits such seizures.[65] In addition, officers can take months, or sometimes years, to search the actual data. The 14-day limit for ordinary property[66] does not apply to electronic files.[67]

Some courts readily admit that permitting agents to seize the entire device amounts to an "over-seizure" that would violate the Fourth Amendment particularity requirement if it involved hard copy documents.[68]

---

61. *In re* 650 Fifth Ave. & Related Props., 830 F.3d 66, 99 (2d Cir. 2016) ("[F]or a warrant to meet the particularity requirement, it must identify the alleged crime for which evidence is sought.").

62. *See, e.g.*, United States v. Williams, 592 F.3d 511, 515 (4th Cir. 2010) (approving a warrant authorizing a search of "[a]ny and all computer systems and digital storage media, . . . documents, photographs, and Instrumentalities" for evidence of the alleged crime).

63. United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013) ("[T]he warrant must specify the 'items to be seized by their relation to designated crimes.'" (quoting *Williams*, 592 F.3d at 519)).

64. United States v. Loera, 182 F. Supp. 3d 1173, 1198, 1214–16, 1237 (D.N.M. 2016) (collecting cases).

65. FED. R. CRIM. P. 41(e)(2)(B).

66. FED. R. CRIM. P. 41(e)(2)(A)(i).

67. FED. R. CRIM. P. 41(e)(2)(B).

68. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) ("We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records,

It is a wholesale, general seizure without any attempt to limit the seizure to relevant documents.[69] Courts excuse this over-seizure on practical grounds, but they then fail at the back end to impose any meaningful limits to the search or inventory to mitigate this over-seizure.[70]

Once courts have granted the agents authority to search the device at all, they are then unwilling to impose limits to the *execution* of the search, with very few exceptions. Courts will impose no search protocols. They will rarely say agents can search in only certain folders or only open certain types of files—such as image files or spreadsheets. Even the Ninth Circuit, which once hinted that a magistrate should, or at least could, impose limiting search protocols has apparently stepped back from that guidance, at least in certain kinds of cases.[71]

Rather, courts almost uniformly approve warrants that allow agents to search any folder or subfolder, any file, any deleted data, any metadata—in short, agents can search anywhere on the device.[72] Sophisticated forensic software generally can uncover almost anything. It is able to identify files that have been mislabeled, hidden, or even deleted. It can piece together disparate scraps of deleted files, and it can uncover metadata showing when files have been opened or modified, when the device has been used for other purposes, and, of course, vast amounts of location data.[73]

The Tenth Circuit has explicated just how broad a search of electronic devices may be. It held that agents may search for evidence of drug crimes in whatever form that might take, from financial documents to "trophy pictures," and look for them in any file type: Word, WordPerfect, Adobe, Outlook, Lotus, Excel, Quicken, Access, or Paradox.[74] The court there drew a conclusion typical throughout the Federal Circuit Courts of Appeal: "[I]n the end, there may be no practical substitute for actually looking in many

---

this will be far more common than in the days of paper records."). *But see* United States v. Schesso, 730 F.3d 1040, 1049 (9th Cir. 2013).

69. United States v. Ganias, 824 F.3d 199, 232 (2d Cir. 2016) (Chin, J., dissenting).

70. *E.g.*, *Schesso*, 730 F.3d at 1042–43.

71. *Id.*; *see also* United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011) (noting that the majority of federal courts take this approach).

72. State v. Goynes, 927 N.W.2d 346, 357 (Neb. 2019); *see* United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009).

73. True, suspects may have encrypted their data—either full disk encryption or particular files. This self-help may limit agents' searches, although in roughly half the cases, some law enforcement agencies can successfully sidestep these protections. N.Y. CTY. DIST. ATTORNEY, REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 2 (2018); OPENTEXT, ENCASE MOBILE INVESTIGATOR 2, *available at* https://www.guidancesoftware.com/docs/default-source/document-library/product-brief/encase-mobile-investigator-product-overview.pdf?sfvrsn=66f569a2_18 [https://perma.cc/EX7N-2DJR] ("Many devices that investigators are faced with are either locked or contain a password. EnCase Mobile Investigator empowers the investigator by offering several built-in bypass functions for select phones so that no evidence within a device can be hidden and unable to access.").

74. *Burgess*, 576 F.3d at 1093–94.

(perhaps all) folders and sometimes at the documents contained within those folders . . . ."[75]

With this broad warrant authority, agents can use or copy any file or information they come across, even if unrelated to the original crime alleged in the warrant. If officers stumble upon an image of child pornography during a search for counterfeiting documents, they may use that image in a prosecution against the suspect for this new crime, or use the image to obtain a new warrant to search for this new crime.[76] Or, if the police come across evidence of gun possession, drug possession or identity theft, they can investigate those crimes too, even if they were not the original crime under investigation. Broad searches do not merely expose innocent information to agents, therefore, but also put suspects in jeopardy for additional criminal charges. And, as in *Wey* and *United States v. Ganias*,[77] agents often keep the information for later data mining.

C. *RATIONALES FOR EXISTING LIMITS*

Courts allow wide breadth for several reasons. First, they analogize to physical searches in the home, where police may look anywhere the object of the search may be found. Second, they subscribe to the myth of the sophisticated user, assuming every suspect employs sophisticated methods to hide files. Third, they point to supposed institutional constraints.

We can challenge each of these rationales in order to strengthen at least *some ex ante* limits on searches; on the other hand, we must also concede that the very nature of paper (and electronic) searches means that officers will always retain broad discretion to search far and wide for evidence.

1. The Home and Chattel Analogy

Courts regularly avow their commitment to protecting the special privacy of papers. They expand upon how electronic devices contain our entire lives, and that courts must be especially vigilant against these searches. The Second Circuit has repeatedly noted that in electronic searches, "the particularity requirement assumes even greater importance."[78] Courts regularly espouse how devices contain "a huge array of one's personal papers,"[79] or "immense amounts of information."[80] "Vast trove" of documents has proven a

75. *Id.* at 1094. The approved search in *Goynes* was similarly broad—basically all files, folders, and metadata—based only upon the officer's assertion that drug dealers often have evidence on their phones, not that this one might. *Goynes*, 927 N.W.2d at 351.

76. United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009).

77. United States v. Ganias, 824 F.3d 199, 217 (2d Cir. 2016); United States v. Wey, 256 F. Supp. 3d 355, 379 (S.D.N.Y. 2017).

78. United States v. Ulbricht, 858 F.3d 71, 99 (2d Cir. 2017) (quoting United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013)), *abrogation recognized by* United States v. Chambers, 751 F. App'x 44, 45 (2d Cir. 2018), *cert. denied*, 139 S. Ct. 1209 (2019).

79. United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009).

80. United States v. Payton, 573 F.3d 859, 861 (9th Cir. 2009).

particularity popular description in the Second Circuit[81]—so vast, that a search of a device resembles a general search of a home.[82]

Despite claiming electronic devices and data should enjoy special treatment, courts immediately follow these avowals with a big "but." But searches of devices are, in the end, no different from a search of a home for contraband such as drugs.[83] Agents do not know where on the device they may find the incriminating document, so they must be allowed to search in every file, every folder, *just as* an officer does not know where she will find drugs, so she can search in every room, every dresser, every drawer. The analogy is compelling—but only if we treat papers as ordinary chattel, or worse, ordinary contraband.

When an officer searches for chattel or contraband, like drugs or a gun, however, she will rarely, if ever, open file folders much less read the contents of the documents. In a paper search, the nature of the item searched *for* compels the type of item that must be searched *among*.[84] A search for drugs in an underwear drawer will reveal underwear—personal but not that important. A search for an incriminating document will reveal all documents, meaning everything personal and private about a person. The justification for broad searches of papers based upon broad searches for contraband in the home only holds if we ignore the courts' repeated protestations that papers and private information are special, more private than other personal belongings.

Nevertheless, these courts do have a point. They correctly note that searches of devices resemble searches of the home in that it is hard to predict in advance where a given document may be found, and agents must read the documents to know what they say. Indeed, the entire reason the founding generation largely banned paper searches was because there is no easy way to find the incriminating document in the haystack without searching through a far greater number of unoffending ones. As a result, as discussed below, almost any attempt to protect Fourth Amendment values through *ex ante* limits only will have limited effectiveness.

2. The Myth of the Sophisticated User

Compounding the above problem, courts often rashly presume that every suspect is a computer mastermind using sophisticated tools to hide or obscure incriminating information. These judges mostly stick to naïve examples: a user who provides a misleading name to a file, such as labelling a contraband

81. *Ganias*, 824 F.3d at 217; *Wey*, 256 F. Supp. 3d at 379.

82. *Ulbricht*, 858 F.3d at 100–01.

83. *Id.* ("Since a search of a computer is 'akin to [a search of] a residence,' . . . searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants." (alteration in original) (citation omitted)).

84. 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.").

image "financial information,"[85] or a suspect who might change the suffix of a file from .jpg to .docx, thus brilliantly throwing investigators off the scent.[86]

We must distinguish different arguments. First, courts worry that suspects will change a suffix, say from .jpg to .xls, to make an image file look like a spreadsheet. Forensic software can easily overcome this naïve alteration. After all, the software cannot open the file into a readable format without first identifying its actual type. Often it can easily do so by examining the first several bytes of the file (rather than the extension).

Second, a suspect may save an image of child pornography in a file folder called "tax documents." This may present a legitimate problem on desktop or laptop computers, though we could still restrict the search to images in that folder. But as I discuss below, the sandbox model of computer programing means that on many mobile devices, users will no longer have access to where files are saved or, in many cases, even the names of files.

Third, some suspects really are computer masterminds.[87] They may alter metadata, for example. Orin Kerr has posited that if law enforcement seeks a document created on a certain date, a suspect may have downloaded the program BulkFileChanger and changed the metadata associated with the file to alter its creation date.[88] He has therefore argued that anything short of a comprehensive search allowing law enforcement to view everything they wish might leave some evidence unrecovered.

But very few suspects meet the description of a person sufficiently sophisticated or motivated to alter files or metadata in a way that would evade even the most basic, off-the-shelf forensic software. Indeed, few suspects will even go so far as to change suffixes or metadata at all. Courts have allowed the very rare prospect of the computer mastermind to drive the entire doctrine, rather than taking the most typical user as the prototype. If the police have reason to believe a particular user has computer expertise, the officers can seek a broader warrant based upon that information.

3. Institutional Constraints

Courts often respond to the argument that warrants should delineate more concrete limits to the scope of an agent's electronic search as follows: Express limits in the warrant would be an *ex ante* limit beyond the *power* of a

85. United States v. Burgess, 576 F.3d 1078, 1093–94, 1093 n.18 (10th Cir. 2009).

86. United States v. Stabile, 633 F.3d 219, 239 (3d Cir. 2011) ("Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer." (quoting United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006))); Thomas K. Clancy, *Fourth Amendment Satisfaction—The "Reasonableness" of Digital Searches*, 48 TEX. TECH L. REV. 37, 45 (2015) ("Professional investigators, however, recognized long ago that computer users attempt to conceal criminal evidence by storing 'it in random order with deceptive file names,' thus, requiring a search of all the stored data to determine whether the warrant includes it.").

87. *See generally Ulbricht*, 858 F.3d (describing the defendant as a skillful computer person).

88. Kerr, *supra* note 12, at 16.

magistrate[89] and beyond a good apportionment of duties.[90] That is, a warrant may only state the things to be seized and the places to search and cannot impose upon agents *how* to execute the warrant.[91]

Besides, courts note they can always review searches *ex post* to determine whether the officers did in fact exceed reasonable bounds in conducting a search.[92] If they ended up searching a jewelry box for a rifle, we can suppress any drugs they found in the jewelry box. These arguments have superficial appeal but suffer from several defects.

First, courts are simply improvising. From the founding until 1967, the Fourth Amendment prohibited searches and seizures of most papers for a criminal case. It is all therefore new. To say magistrates lack the constitutional power cannot rest on any well-settled principle.

Second, even as to physical world searches, magistrate judges can and do state limits in advance governing where within a residence agents may search when magistrates know in advance the nature of the premises.[93]

Third, the Fourth Amendment itself casts doubt on courts' unwillingness to impose meaningful search limits. We must remember, courts authorize agents to seize the entire device, an unlawful over-seizure under the Fourth Amendment. It is likely true we must excuse this violation for practical reasons, but that does not mean we should ignore the continuing taint of the over-seizure. Rather, we should consider any future searches to be part of that continuing over-seizure.[94]

Fourth, courts never learn the extent of the search for any *ex post* review. Rather, they only learn of those incriminating files that the prosecutor has used to investigate or charge the defendant. Everything else agents look at

89. *See generally* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010) (arguing *ex ante* search protocols are unconstitutional).

90. *In re* Search Warrant, 71 A.3d 1158, 1168–70 (Vt. 2012) (summarizing the *ex ante*/*ex post* debate and approving *ex ante* limits).

91. *In re* A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 396 (S.D.N.Y. 2014).

92. Warshak v. United States, 532 F.3d 521, 528 (6th Cir. 2008).

93. *In re* Search Warrant, 71 A.3d at 1170 ("Even in traditional contexts, a judicial officer may restrict a search to only a portion of what was requested—a room rather than an entire house, or boxes with certain labels rather than an entire warehouse."). This is particularity true of search warrants for businesses that will limit a search to one office but not another, even though both occupy the same premises. State v. Matsunaga, 920 P.2d 376, 380–81 (Haw. Ct. App. 1996). The problem is not so much power but knowledge. Magistrates cannot list limits beforehand because they have traditionally not known where agents would need to look.

94. United States v. Ganias, 824 F.3d 199, 232 (2d Cir. 2016) (Chin, J., dissenting). Orin Kerr has argued that the continuing seizure concept arising out of the original over-seizure should prohibit agents from *using* any documents found to bring more charges or seek a new warrant for new crimes. Kerr, *supra* note 12, at 5. I would simply use this same idea of continuing seizure to justify, based on the Warrant Clause itself, limits to the scope of the agents' search back at the lab. The Ninth Circuit took this approach in its guidelines in *United States v. Comprehensive Drug Testing, Inc.*, justifying *ex ante* search protocols by linking the later search of the device with the earlier over-seizure of all the device's contents. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

remains obscured from court and defendant alike. My inventory proposal will, of course, remedy this deficiency.

Finally, the Supreme Court has built several layers of deference into any *ex post* review. Reviewing courts must defer to an officer's search because, ironically, the officer had relied upon a warrant;[95] they must defer because it *is ex post* and courts are reluctant to second guess officers;[96] they must defer because the practical effect would be to suppress evidence in a criminal case, which courts are often reluctant to do—indeed, they must do their best to sever the portion of the warrant that is not tainted;[97] they must defer because the good faith doctrine tells us that unless the officers were reckless, their reliance on a warrant insulates them even if they violated the Fourth Amendment.[98] These same principles of deference will apply even in a civil case, because qualified immunity protection for officers parallels the good faith doctrine for the exclusionary rule.

In sum, courts say it's too hard to impose limits *ex ante* and refuse to impose any meaningful *ex post* limits. *Ex ante* is too hard because a court cannot predict where to look, while *ex post* counts as second-guessing. In addition, courts treat the only available *ex post* remedy as reviewing the warrant itself to determine whether the officers' execution of the warrant followed its liberal scope. What they do not consider as an *ex post* remedy is the inventory I propose below.

III. SANDBOX APPS AND *EX ANTE* LIMITS TO SEARCHES

In this Part, I turn to how we may enhance *ex ante* limits given recent changes in device operating systems. This proposal will promote privacy-as-secrecy—limiting where officers may actually look. Later, I turn to my *ex post* remedy that helps to enforce other central Fourth Amendment goals of security through the inventory requirement.

Recent developments in data privacy and security have begun to radically change how devices store files, and these changes should limit how officers search devices. Once, users controlled where they stored files, and had direct access to the file directory. Now, as any iPhone or Android user can tell, users no longer determine where an app stores its files, because users have no direct access to the file directory.[99] As a result, files are stored in predictable places.

---

95. Illinois v. Gates, 462 U.S. 213, 236 (1983) ("A magistrate's determination of probable cause should be paid great deference by reviewing courts." (internal quotation marks omitted) (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969))).

96. *Id.*

97. United States v. Galpin, 720 F.3d 436, 448–49 (2d Cir. 2013) (noting courts should sever the invalid portions of a warrant to save evidence seized under valid portions to avoid the "harsh medicine" of the exclusionary rule (quoting WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.6(f) (5th ed. 2019))).

98. *See, e.g.*, Davis v. United States, 564 U.S. 229, 250 (2011).

99. *File System Programming Guide*, APPLE, https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html [https://perma.cc/XZG6-6826]; *Permissions Overview*, ANDROID,

This evolution represents a sea-change in computer science and security. In the 1970s, the model that prevailed was the "user as program" model.[100] Each program had all the privileges of the user. Security was understood as distinguishing between users and segregating between users (even if on the same server), but not segregating between functions or programs a single user used. Similarly, programs either had all permissions and privileges or none.

Developers now follow a "principle of least privilege." This principle applies to each app or function, rather than to each individual user.[101] Each app has its own sandbox[102]—an assigned folder and set of subfolders. The app works almost entirely within this sandbox. It keeps most necessary files and databases within this enclosed set of folders, and it stores any new files the user may create here.[103]

In addition, the smartphone operating system will enforce segregation between these apps. One app ordinarily will not be able to share data with another; one app will not be able to invade the sandbox of another. Of course, apps often need data from other apps, but smartphones will carefully regulate any such interactions as if each app were a separate user requesting limited information from another. And the individual (human) user must have previously approved this particular app obtaining information from another app.

For agents searching mobile devices such as smartphones or tablets, this sandbox model means that we can more easily impose *ex ante* limits, whether in the warrant or by voluntary protocols developed by law enforcement. In a drug case, for example, if the police have probable cause to believe the suspect has used his phone to send messages concerning drug deals (because they saw him use it), those officers may search only messaging apps. The sandbox regime means that it is very unlikely messages will be stored in some secret, hidden location. Ordinary users do not have the access or the power to save messages anywhere other than within the file structure of the app's sandbox.

This sandbox limit supplements and elaborates efforts by some courts and scholars to impose more meaningful *ex ante* limits. Adam Gershowitz has proposed numerous ways in which magistrate judges can issue warrants that impose greater limits to the scopes of searches.[104] Courts should, and increasingly do, limit searches to information within a particular timeframe.[105]

---

https://developer.android.com/guide/topics/permissions/overview [https://perma.cc/4VCW-S2EG].

100. *See generally* Dennis M. Ritchie & Ken Thompson, *The UNIX Time-Sharing System*, 17 COMM. ACM 365 (1974) (typifying the "user as program" model prevailing in the 1970s).

101. *Cf.* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 586 (2018) ("By imposing these restrictions, sandboxes both conform to and inform a user's expectations about security and privacy.").

102. *See id.*

103. *File System Programming Guide*, *supra* note 99.

104. Gershowitz, *supra* note 10, at 629–38.

105. Wheeler v. State, 135 A.3d 282, 304 (Del. 2016) ("Federal Courts of Appeals have concluded that warrants lacking temporal constraints, where relevant dates are available to the

As for those documents otherwise innocent and kept by most individuals and businesses, such as financial records, courts require greater specificity and link to the alleged crime.[106]

Gershowitz has also argued that officers should state with greater particularity the evidence they have probable cause to believe resides on the device and obtain a warrant to search for that type of information only. For example, if officers in a drug case assert that the defendant used his phone to communicate with other drug dealers, those officers should be limited to searching the phone for communications only. By contrast, currently, once officers have probable cause to believe the defendant has committed a drug offense, they may search the phone anywhere for any evidence of drug crimes.[107] Additionally, it is very easy for officers to establish probable cause. Courts routinely find probable cause merely based upon the nature of the crime, such as drug trafficking or even possession, without any fact tying the crime to the device to be searched.[108]

He and others have also analogized imposing greater *ex ante* limits similar to those found in the federal and state wiretap law.[109] These limits impose higher showings to justify a wiretap, such as exhausting alternatives, and express minimization procedures, including a 30-day time limit and limits on listening only to relevant conversations.[110]

* * *

We may draw two lessons from our survey of *ex ante* limits, both of which support my inventory proposal. First, even with enhancements, *ex ante* limits may not be enough. In the end, the nature of a paper search will entail the right and need for officers to sift through a large number of innocent files to find the one they seek. We need the inventory to round out protections, especially other rights to be secure beyond privacy-as-secrecy. The inventory will afford individuals some measure of knowledge and control over that search.

But to the extent we enhance *ex ante* limits far more robustly, so that they resemble the limits in the Wiretap Act, for example, an inventory requirement will become all the more important as an enforcement mechanism, allowing the court and suspect to determine independently that the officers abided these enhanced limits of the warrant.

---

police, are insufficiently particular.") (collecting cases); *see* People v. Thompson, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019).

106. United States v. Wey, 256 F. Supp. 3d 355, 380–82 (S.D.N.Y. 2017).

107. Moats v. State, 168 A.3d 952, 964–65 (Md. 2017) (holding that a drug crime that involves other persons is sufficient to infer evidence on cell phone and permitting exhaustive search and citing cases).

108. United States v. Garay, 938 F.3d 1108, 1113–14 (9th Cir. 2019) (holding probable cause finding proper merely because a person was arrested in a car with guns, drugs, cash, and a cell phone—no direct evidence that the phone would contain evidence of the crime).

109. *See, e.g.*, 18 U.S.C. § 2518 (2012); CONN. GEN. ST. § 54-41c-k (2019).

110. 18 U.S.C. § 2518; CONN. GEN. STAT. § 54-41c-k.

IV. MY PROPOSAL: "TO BE SECURE" VIA AN INVENTORY

This Section sets forth my proposal. Most discussions of limiting searches of electronic devices, as detailed above, focus on *ex ante* protections—that is, preventing officers from opening and viewing files in the first place.[111] They focus on privacy-as-secrecy only—the notion that privacy protects the secrecy of information only and not other values, such as an individual's right to understand who has seen the personal information or to control how it is used. These discussions therefore ignore the key Fourth Amendment value actually protected: security. This Article proposes a solution that furthers security via the particularity requirements governing the inventory and return of the warrant. Security includes not only privacy over what officers see but also security in the sense of control by and transparency to the individual —values we must protect *ex post*, after the warrant has issued and the search and seizure have occurred.

This Section briefly considers current law on inventories for electronic files. It then details my proposed inventory requirement. It next provides reasons in support that rest both upon policy grounds as well as Fourth Amendment principles.

A. CURRENT LAW FOR INVENTORY FOR ELECTRONIC DEVICES

Federal Rule of Criminal Procedure 41, as well as its state analogues, requires officers to execute a warrant within 14 days, to create an inventory of every individual thing they seize, and to provide this list to the suspect immediately as a receipt and provide the list to the court "promptly" as part of the return.[112] As discussed in Part VI, cases, statutes, treatises, and practice have required an inventory for centuries. Additionally, all or nearly all states require inventory today, and it should likely be viewed as required by the Fourth Amendment.

Unfortunately, most courts do not apply the foregoing inventory principles to searches of electronic devices in any meaningful way, robbing the particularity requirement and the Warrant Clause of its force almost entirely. Courts,[113] Rule 41,[114] and actual practice[115] all permit officers to list the device on the inventory only, and not the files opened and viewed. A

111. *E.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1172–73 (9th Cir. 2010) (explaining its protocols seek to limit what the investigating officers view); Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 135–37 (2017) (canvassing use restrictions (not including an inventory) and arguing in favor of *ex ante* collection limitations); Gershowitz, *supra* note 10, at 591–92.

112. FED. R. CRIM. P. 41.

113. United States v. Pawlak, 237 F. Supp. 3d 460, 470 (N.D. Tex. 2017).

114. FED. R. CRIM. P. 41(f)(1)(B) ("In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied.").

115. *See* United States v. Wey, 256 F. Supp. 3d 355, 383 (S.D.N.Y. 2017).

typical inventory will simply say, "HP Presario CQ60 Laptop," or "3 USB sticks."[116]

B. INVENTORY, RETURN, AND RECOVERING OF PROPERTY

I propose a vastly different regime, one far more consistent with the principles underlying the Warrant Clause and the particularity requirement. I propose that in executing the warrant, law enforcement must provide the court and suspect an inventory of all files opened or looked at during the search of the device. The warrant must also separately list files individually copied. Finally, I provide more robust opportunities for restoring the property to the defendant or suspect by requiring that law enforcement delete its copies almost immediately.

First, the inventory: Within 14 days, law enforcement must complete its search of the device (i.e., execute the warrant) and create an inventory listing the folders opened and searched, the files opened and viewed, and the files (or folders) copied. Luckily, forensic software should make this accounting process automatic: Agents will merely need to generate a report that will list all the files and folders opened. Officers will provide this inventory to the suspect and the court.

Courts will sometimes need to grant officers extensions of the 14-day limit because of limited law enforcement resources. But these courts should remain involved in limiting the length of time law enforcement seeks to keep and search a person's device. After all, seizing an entire device seizes files and data that are *not* responsive to the warrant, and this "over-seizure"—in a sense a continuing Fourth Amendment violation—should last no longer than necessary.[117]

Second, my rule will also require restoring the information back to the individual in a timely fashion. Law enforcement may copy any incriminating evidence, as long as it provides a list of those files to the suspect or defendant, as noted above. But otherwise, law enforcement must give back all other files, and delete its own copies of these innocent files. In this way, we treat the files and data as property. Like the cash in the above scenario, a suspect is entitled to receive the files back if those files are innocent. This procedure will rule out later data mining of the entire disk.[118]

Third, in the idealized physical world, the suspect observes the police carrying out the search and seizure. This allows the person to confirm that the police are acting within the authorized scope of the warrant. True, the suspect or defendant will have little to no power to effectively object to any

116. Inventory Form, United States v. 7818 NE 91st Ave, No. 3:18-mj-05224 (W.D. Wash. Oct. 5, 2018); *see* Inventory of Items Seized, United States v. Hyatt's Suboxone Clinic, No. 5:18-mj-00047 (W.D. Va. Aug. 20, 2018) ("Laptop labeled as S1RAC1 (Acer N15Q9 . . .)"); *see also* Evidence Recovery Log, United States v. 112 Kentucky Drive, No. 1:18-mj-09194 (N.D. Ohio Oct. 4, 2018) ("black HP laptop"); Return; Receipt, Inventory of Search Warrant, United States v. 1030 Mason Street NW, No. 4:18-mj-06155 (N.D. Ohio July 26, 2018) ("IPHONE w/ TAN CASE").

117. United States v. Ganias, 824 F.3d 199, 232 (2d Cir. 2016) (Chin, J., dissenting).

118. *Id.*

violation in real-time. Nevertheless, courts from *Entick* to *Groh* seem to envision the suspect's observing the search to reassure herself that the officers act within the scope of the warrant; the observation alone may have the effect of limiting the search. And, of course, if a suspect simply says, "This is not my bedroom, this is someone else's," officers are very likely to abide by that limit absent contrary information. For example, in the *Wey* case, Michaela Wey, the defendant's wife, was present during the search. She told the officers which were the children's bedrooms and urged the officers to hurry. In fact, the FBI told the court they conformed their search to some of her requests.

Can we apply this principle of observation to the digital world? Perhaps. We might require or allow, in appropriate cases, suspects or counsel to personally observe the device search. Now most counsel would not permit their clients to participate in a search in the sense of explaining to agents how they organize their files—for self-incrimination reasons. But counsel might choose to participate, as they do at line-ups, in the device search to further ensure law enforcement abides by the limits of the warrant. I do not place too much emphasis on this suggestion because it seems impractical and perhaps extreme, even if it does parallel a similar requirement in the physical world.

A more practical analogy to the suspect's observation of a physical search would be to require law enforcement to provide all search queries it used in addition to an inventory of the files it actually opened. I similarly do not place much emphasis on this proposal. After all, search inquiries are as likely to reveal law enforcement techniques, or attorney work product, as any useful information for a defendant once he already has a list of all the files opened.

* * *

I have limited my proposal to devices, but many of my arguments apply with some adaption to third-party subpoenas or warrants from electronic providers. For example, law enforcement serves millions of subpoenas or warrants on providers for a person's emails, messages, social media accounts, posts, photos, location data, and other information kept by various types of third-party providers such as internet providers and social media platforms.[119]

These warrants or subpoenas on third parties raise a myriad of questions about notice under the Stored Communications Act and other provisions. For warrants, law enforcement does not need to provide any advanced notice to an account holder, beforehand or afterwards, much less provide the account holder an inventory of the information obtained or viewed. Subpoenas require advance notice of the demand, but they do not appear to require any subsequent inventory either.

We can see how my proposal applies quite naturally to this arena as well. Law enforcement should be required to make an accounting of the files,

119. *E.g.*, *United States Report: Law Enforcement Demands for Customer Data—United States*, VERIZON WIRELESS, https://www.verizon.com/about/portal/transparency-report/us-report [https://perma.cc/WMR3-4SRS] (reporting that Verizon received 284,407 warrants, subpoenas, and other legal process in 2018).

emails, or other information they obtain, the information they actually look at, and a requirement for the distribution of this copy to a suspect, defendant, or witness in a reasonable amount of time.

C. REASONS JUSTIFYING MY PROPOSAL

Below I consider several reasons to require an inventory for electronic files, including especially the value of the inventory in furthering a person's right to be "secure" in her "papers." The inventory affords the individual understanding and control over her data, it imposes upon law enforcement few practical obstacles or additional burdens, and it helps to supervise searches to reduce, as a deterrent, the scope of searches in the first place.

1. Original Understanding (Deferred)

The founding generation understood warrants to require an inventory. This understanding is emphasized in founding era statutes, case law, and justice of the peace manuals. I argue this understanding became part of the Warrant Clause of the Fourth Amendment, but I defer this important argument to Part VI because of its length and special character.

2. To Be Secure

The Fourth Amendment right "to be secure" in one's papers includes numerous sub-rights. Of course, it includes the right to secrecy, and the (limited) *ex ante* protections, above, help protect privacy-as-secrecy from any outside prying eyes. At the inventory stage, however, we assume officers have already viewed the items.

Beyond privacy-as-secrecy, the right to be secure overlaps considerably with protections that are often ranked as aspects of privacy considered more generally. The terminology does not matter much, but the Fourth Amendment uses the term "secure," and this term better embraces protection for data than does the term "privacy." I will use the term "secure" though often draw, for its particulars, upon the privacy literature, as well as data security sources.[120] For example, privacy law and data security draw heavily upon the Fair Information Practices ("FIPs"), "the building blocks of modern information privacy law."[121] These include principles such as transparency, data minimization, and use limitations.

Many data privacy laws and rights center on mass data collection by government agencies or private entities, such as retailers or internet platforms. In drawing upon these sources, we must recognize differences that arise in the context of law enforcement executing search warrants. For example, in the context of mass data collection, privacy principles emphasize

120. *See generally* Cohen, *supra* note 24 (discussing privacy and its relation with systems of surveillance); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 522 (2006).

121. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999); *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1824–25 (2011); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 908 (2009).

the right to choose and to consent. In the law enforcement context, suspects enjoy little right of choice or consent once a warrant has been issued.

On the other hand, we can adapt many of the rights from the mass data collection arena to our situation. Doing so will provide language and concepts for what it means for an individual to be secure in her data that has been seized by the government. I have therefore drawn loosely upon state and federal statutes, the EU General Data Protection Regulation,[122] and scholarship below.

To be secure includes the following sub-rights or at least interests. It includes transparency: The individual knows what files officers have viewed and what they have not. Transparency also means the individual understands how her data are being used. To be secure includes data minimization: The government collects and, more importantly here, views, only what is necessary, and it destroys data it no longer needs—either automatically or upon request.[123]

To be secure includes ordinary data security: The government takes steps to keep the data safe from outsiders such as hackers and notifies the individual if there is a breach. Nearly every state has passed data breach laws that require companies to notify consumers when their data have been stolen by a hacker, including the particular data taken.[124] It includes the dignitary right to control data.[125] Finally, it includes the right against anxiety over how the data may be used beyond the initial collection effort and anxiety over breach.[126]

California's new Consumer Privacy Act[127] focuses primarily on data collection by internet platforms—such as Facebook or Google—but its principles also help in the warrant context. California's Consumer Privacy Act

---

122. Commission Regulation 2016/679, 2016 O.J. (L 119) [hereinafter GDPR].

123. Schwartz & Solove, *supra* note 121, at 1880; *cf.* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012) (discussing the potential right of internet users to have their data and pictures purged from certain social network websites); *Internet Law—Protection of Personal Data—Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request.—Case C-131/12*, Google Spain SL v. Agencia Española de Protección de Datos *(May 13, 2014)*, 128 HARV. L. REV. 735, 735 (2014) (arguing that the Court of Justice of the European Union was correct to hold that a Directive meant to regulate data controllers created a presumption that Google has to delete links to personal information if requested to do so by a data subject).

124. Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 428 (2015) ("[N]early every state has enacted breach-notification laws, and there is a push for federal legislation on the topic.").

125. Solove, *supra* note 120, at 522 ("The harm is a dignitary one, emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives.").

126. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016) ("In addition, a blood test, unlike a breath test, places in the hands of law enforcement authorities a sample that can be preserved and from which it is possible to extract information beyond a simple BAC reading."); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 745 (2018) ("Knowing that thieves may be using one's personal data for criminal ends can produce significant anxiety.").

127. California Consumer Privacy Act, ch. 55, 2018 Cal. Legis. Serv. 1809 (West) (to be codified at CAL. CIV. CODE § 1798.100).

provides individuals with a right to know what information data platforms collect and why.[128] Individuals can request data be deleted.[129] Individuals can also obtain the data collected in a "readily usable format."[130] These rights create strong transparency, data minimization, and individual control over data.[131]

As for the right against anxiety, we may also note that the Supreme Court has recently recognized such a right.[132] It might seem a mere psychological vulnerability, but the literal etymology of "secure" comes from the Latin "care free." Now often etymology is a poor substitute for reasoning, but "secure" truly does retain this notion of "without care." Anxiety over government possession, use, and data mining of a person's entire digital life creates tremendous anxiety and therefore counts as the opposite of secure.

The Supreme Court has recognized this "anxiety" interest as protected by the Fourth Amendment, at least in passing, in *Birchfield v. North Dakota*.[133] The Court noted that law enforcement must obtain a warrant to draw blood from a driver suspected of drunk driving.[134] The Court required a warrant after balancing the intrusion upon the defendant's privacy against the government's interests in law enforcement.[135] On the privacy side, the Court noted that a person would feel "anxiety" knowing that the government had a sample of his blood, and the government could use that blood sample any way it wished beyond testing it for alcohol.[136] It could test the blood for DNA later to see if it matched a database of unsolved crimes. It could also test the blood for drug use, even though there was no probable cause initially to do so.

The inventory requirement I propose will further these protections. First, this inventory will afford an individual security and privacy through transparency. She will not need to guess whether law enforcement looked at medical records, family photos, embarrassing or private sexts or romantic emails. She will know precisely which items law enforcement did or did not access.

Second, the individual will understand how her data are used and, as particularly relevant here, why law enforcement has the legal authorization to access those files. In other words, she can compare the files viewed against the

128. *Id.* § 3.

129. *Id.*

130. *Id.*

131. *Id.* § 2(g)–(i).

132. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016).

133. *Id.* ("Even if the law enforcement agency is precluded from testing the blood for any purpose other than to measure BAC, the potential remains and may result in anxiety for the person tested."); *see also* Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1, 3 (2018) ("[T]he Court embraced a proposition that has long eluded Fourth Amendment law: that 'anxiety' about the misuse of already-collected information can be reasonable, and can merit constitutional accommodation, *even if* the misuse is 'precluded' by other legal obstacles.").

134. *Birchfield*, 136 S. Ct. at 2184–85.

135. *Id.*

136. *Id.* at 2178.

items described in the warrant to ensure law enforcement has acted within its scope.

Third, my proposal requires the government destroy its copies of unneeded information within 14 days or some other limited timeframe. This furthers the data minimization principle, and the security principle. If the government no longer retains the data, outsiders cannot breach it.

Fourth, the inventory will promote security and limit a person's anxiety over what the government has seen, accessed, or copied in the short term. It will also promote security by requiring the government to destroy any information it does not copy and need. This requirement assures individuals that the government will not continue to use their data for mining purposes or to search for new crimes.

Indeed, law enforcement often retains a suspect's digital data long after the initial warrant and seizure in order to perform later searches or data mining, sometimes for entirely new crimes. Courts have disapproved these practices,[137] though not always deeming them unlawful.[138] My proposal would make such subsequent, long term data mining impossible by requiring the prompt destruction of most of law enforcement's copy of the suspect's data.

In addressing the harms of digital searches, scholars rarely recognize these other aspects of the right to be secure because those scholars too often focus on the right of privacy-as-secrecy, the right merely to avoid officers viewing the files in the first place. This focus leads us to fiddle endlessly with *ex ante* solutions that will forever evade us. For example, Orin Kerr once argued a suspect does not need an inventory for the individual files on her device because she should already know the files that are on her own device.[139] This may have been true when he wrote, but of course today suspects probably do not know the vast range of files, metadata, or other information on their devices. But more to the point, the suspect does not care so much about which files are on the seized device but rather, which files law enforcement has viewed. Did officers view family photos, naked pictures, sexts, love letters, diaries, personal texts, or did they properly restrict themselves to opening just tax documents? This difference matters, even though law enforcement has initially seized all of the files when they seized the device.

---

137. *See* United States v. Hulscher, No. 4:16-CR-40070-01-KES, 2017 WL 1294452, at *14 (D.S.D. Feb. 10, 2017) ("[L]aw enforcement agencies are free to share information among themselves and are not required to purge the evidence in their possession once a case is completed."). *But see* United States v. Wey, 256 F. Supp. 3d 355, 405 (S.D.N.Y. 2017) (finding a violation of the Fourth Amendment because "the Government evinced no hesitation to subject the electronic Search fruits to continuing and, at least to some extent, expanding searches as its investigation and charging theories developed over the months and years following the initial Searches").

138. *See* United States v. Ganias, 824 F.3d 199, 224–26 (2d Cir. 2016) (concluding that agents acted reasonably and in good faith in relying on a 2006 warrant).

139. Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 104 (2005).

More recently, Kerr has written that a seizure occurs only when law enforcement uses items to seek further criminal charges.[140] This view at least recognizes that some files on the device matter more than others. I simply disagree. Again, viewing matters to most people's privacy and security, whether the viewed contents are used for criminal charges or not.

3. Rule of Law

In *Groh v. Ramirez*,[141] the Court illustrated many of the rule-of-law principles undergirding the Warrant Clause. Drawing upon that case, I construct a hypothetical scenario below to show how the inventory makes a person secure in her papers.

Under this hypothetical but common scenario, officers obtain a warrant and must execute it within 14 days. They arrive at the home of a suspect who shares a house with two roommates. The officers show the warrant to the suspect. The warrant says that the officers have probable cause to believe the person has violated drug possession and distribution laws. It also says the officers have probable cause to believe the suspect possesses, in his home, cocaine, scales, baggies, and cash derived from drug sales, and that they may seize these items.

The suspect reads the warrant and understands the lawful authority for the search. He understands that a magistrate has reviewed the evidence and independently concluded that there is probable cause to believe he has committed a crime and probable cause to believe he possesses these items. He also understands that the officers are authorized to enter the premises and seize the items listed. The list is particular, and the suspect understands exactly what the officers may seize. The list is also particular enough to rule out arbitrary enforcement by the officers—"scales," for example, leaves the officer little discretion.

The officers search the living room. They ask him which bedroom is his, and he tells them. The suspect's two roommates who are present are protected because the officers cannot, and do not, search their bedrooms. In the suspect's bedroom, they search anywhere one might find cocaine.[142] But they do not rip open upholstery, for example, because they lack probable cause in this case to believe the suspect has gone to those lengths to hide the cocaine.

The officers do not find cocaine or baggies, but they do find a scale, scissors, and $150 in cash, all of which they take. They list the scale, scissors, and the $150 and leave this list with the suspect as a receipt. The officers also promptly provide the court with an inventory of what they have seized as part of the return.

---

140. *See* Kerr, *supra* note 12, at 25–26 (proposing a Fourth Amendment rule that "subsequent use [of seized data] renders the ongoing seizure unreasonable").

141. Groh v. Ramirez, 540 U.S. 551 (2004).

142. Officers may search "the places in which there is probable cause to believe that [the thing] may be found." California v. Acevedo, 500 U.S. 565, 580 (1991) (quoting United States v. Ross, 456 U.S. 798, 824 (1982)) (noting that this is the rule with or without a warrant).

In the founding era, though not today, a court would physically compare the items seized with the list in the warrant, or compare the items listed in the written inventory with the items listed in the warrant. Rule 41 does not require such a time-consuming procedure. Rather, Rule 41 envisions suspects enforcing the comparison. Suspects receive both a receipt and the inventory, and they may move to have their property returned.

The suspect files a motion under Rule 41 for return of the cash and scissors. The court holds a hearing and determines whether the items seized match the items listed in the warrant (or were seized under an exception to the warrant requirement such as plain view).[143] Scissors are not listed on the warrant, are not plainly contraband, and so they must be returned to the suspect. The court finds insufficient evidence that the cash came from drug sales, so it orders the cash be returned to the suspect as well. The court allows the police to keep the scale pending any charges but keeps them on a short leash. If the government does not bring charges within a short period, the court will order law enforcement to return the scale as well.

This paradigm flows almost directly from the comments in *Groh v. Ramirez*.[144] There, the court held that a warrant must list the items to be seized with particularity, and a failure to do so may not be cured by such a list appearing in the affidavit the officers submitted to the magistrate in seeking the warrant (unless expressly incorporated).[145]

The Court in *Groh* insisted that the warrant itself list the items for several related reasons. First, the warrant would assure the person subject to search that the officers were authorized to search the places they seek to search and to seize the items they seek to seize.[146] It would also limit their discretion to those items, preventing them from seizing other items not listed (and not contraband in plain view).[147] From the *Entick* and *Wilkes* cases, we can also draw two important inventory principles: A person is entitled to know and understand what property was taken, and a person is entitled to have the power to get it back. These cases also stress the importance of the timely return of the warrant to the court, so the court can ensure the warrant was carried out quickly and properly.

Most state rules and Federal Rule of Criminal Procedure 41 codify these principles. Rule 41 requires officers show the suspect the warrant.[148] It requires them to leave the suspect a receipt listing what they took.[149] It requires them to provide the court an inventory of what was taken in a return

143. *See generally* Horton v. California, 496 U.S. 128 (1990) (describing the scope of the plain view doctrine).

144. *See generally Groh*, 540 U.S. 551 (documenting an analogous process).

145. *Id.* at 559–60.

146. *Id.* at 561.

147. *Id.* at 560–61.

148. FED. R. CRIM. P. 41(f)(1)(C).

149. *Id.*

on the warrant promptly.[150] Finally, Rule 41 affords suspects the right to get their property back under certain circumstances.[151]

We can see how many of these principles from the physical world support the reasons adduced above for the electronic. For example, suspects will be able to confirm that law enforcement largely abided by the scope of what the warrant authorized. Suppose in a tax fraud case the warrant authorizes officers to search a person's device for files evidencing large expenditures. After the search, the inventory shows that the officers opened and copied a few family photos in which the family were aboard a recently purchased yacht. In this case, the suspect will have little grounds for complaint.

On the other hand, if the inventory reveals that law enforcement opened personal emails between a mother and daughter in 2016 bearing no relation to tax fraud from 2012, the suspect will have grounds to lodge at least an informal complaint and perhaps, a right to sue for a Fourth Amendment violation under Section 1983.

4. Practicality

The inventory proposal here should impose few burdens on law enforcement—fewer burdens even than the existing inventory requirement in the physical world. Indeed, those cases addressing inventories of physical papers and files often hold that the inventory for those types of cases need be no more specific than provided because it would be impracticable for officers to prepare a detailed inventory within the required timeframe.[152]

By contrast, for most files, forensic software will be able to produce reports and inventories automatically. For more complex files or databases that contain so much information that we will want to limit law enforcement only to sub-sets of these files or databases, the forensic software should likewise be configurable to automatically track the actual data sought and viewed. The software could keep a log of database queries, for example. Or the native software could keep a running log. Or, finally, the agent herself could simply write down the breadth of data. For example, she could write down that she read all text messages between the suspect and Person A during a certain limited time period.

Moreover, this inventory can be specific while the warrant itself often cannot be. That is, a warrant can only list items by type because officers do not know what they will encounter. Therefore, officers need only describe in the affidavit and magistrates need only describe in the warrant categories such as "all tax records from 2012." After the search, however, officers can obviously specify the precise files they opened or copied (or the software can).

150. FED. R. CRIM. P. 41(f)(1)(B), (D).

151. FED. R. CRIM. P. 41(g).

152. United States v. Birrell, 269 F. Supp. 716, 722 (S.D.N.Y. 1967) (seizing millions of documents).

5. Section 1983

Currently an individual learns about the scope of a law enforcement search of digital devices almost entirely based upon the incriminating files agents find and use against her. In other words, law enforcement may open and view thousands of files, or more, but a suspect will only learn about the handful that are incriminating. Agents may open files from folders or apps that have nothing to do with the case, and the individual will never find out because no incriminating files were found in those particular folders or subfolders.

My inventory requirement will cure that ill, and individuals will now have a full accounting of the scope of the search. If the search exceeds the scope authorized by the warrant, for the first time, individuals will be able to bring a Section 1983 action for a remedy. In an ordinary physical search of the home, for example, an individual can sue officers for exceeding the scope because they personally observe the search and its scope.[153] Indeed, the cognate trespass lawsuit was originally the main or sole enforcement mechanism for bad searches.

6. *Ex Post* Becomes *Ex Ante*

As noted above, courts have almost entirely refused to impose *ex ante* limits on law enforcement searches of devices. A warrant that lists the category of files and the device or type of device is particular enough. I have sketched above some suggested ways to impose *ex ante* limits consistent with the particularity requirement of the Warrant Clause, but here I show how the *ex post* limits of an inventory, receipt, return of the warrant, and return of the property will evolve into *ex ante* limits.

First, agents who know they must turn over to suspects and the court a list of every file they open will naturally try harder to limit their searches. Second, when those lists reveal searches that went too far, suspects can sue under Section 1983, and courts can suppress evidence in the criminal case. These two factors will provide an *ex post* remedy but also impose in the future a deterrent effect on officers aware of these potential remedies; the remedies will therefore enhance protections *ex ante*.

Third, in any suppression motion or Section 1983 case, courts will begin to develop more nuanced principles for what counts as an overbroad search because they will have, for the first time, a comprehensive list of all the files searched. Under the current practice, all that courts and suspects know are the files searched that also are incriminating. If more suspects sue for overbroad searches, courts will have fuller records of the details of those searches that they can include in their opinions. This transparency from individual cases will aggregate into a far broader, methodical view of how searches of devices really work.

---

153. *E.g.*, Opalenik v. LaBrie, 945 F. Supp. 2d 168, 178–79 (D. Mass. 2013) (discussing the homeowner who witnessed and complained to officers for searching beyond scope of the warrant and later sued under Section 1983).

Fourth, forensic software makers such as Encase and Cellebrite will incorporate the case law and any protocols law enforcement develops to effectively limit searches. Right now, Encase and other makers largely advertise and configure their software to maximize the scope of searches so that law enforcement does not miss anything. After all, law enforcement buys the software—not suspects. But if law enforcement begins to develop limiting principles and protocols, they will insist that Encase and others build these principles into the software.

For example, Encase currently advertises OCR (optical character recognition) as a way to expand the search, to find text in pictures that might be incriminating.[154] But of course, OCR can be used to limit searches too, by putting out of bounds all images that do not contain text, for example. As the sandbox model comes to dominate devices, forensic software should provide options to limit searches to those apps already determined to contain certain types of information. If police have probable cause to believe a drug dealer used his phone for messaging others, the forensic software can provide just messages—from only those apps that create messages. Agents will have no justification to range over the entirety of the device, and the forensic software will impose that limit. If an officer exceeds that limit, the software will make a record that will be included in the inventory provided to the court and the individual.

In this way, the inventory performs precisely the enforcement mechanism it always has. Its matching function makes the *ex post* remedy an *ex ante* protection. Officers know from the start of their search that someone—judge or individual—will compare where they search and what they seize by means of the inventory with the warrant's authorization. This knowledge in turn will encourage officers to observe limits on their searches.

Finally, the requirement that law enforcement return and destroy any data it does not copy as relevant will also act as an *ex ante* limit in the most effective way. If law enforcement no longer has the data, it cannot perform new searches to find new crimes.

7. Wiretap Laws

State and federal wiretap acts provide strong support for my inventory proposal by analogy.[155] These acts and the courts construing them routinely emphasize that wiretaps are extraordinary intrusions upon privacy that must therefore include strict safeguards, just as courts regularly avow the sacred privacy of electronic files. Many of these wiretap acts have what is essentially an inventory requirement of all the conversations a wiretap will potentially scoop up. Law enforcement may only listen to and record those that are described in the warrant, and they must cease listening to or recording others.

Law enforcement must return the recordings to the court, and, in some states, make the recordings available to the individual. The recordings are a

154. OPENTEXT, *supra* note 73.

155. 18 U.S.C. §§ 2510–2521 (2012); CONN. GEN. STAT. §§ 54-41a to -41u (2019).

subset of all the calls intercepted, just as the files opened and viewed by law enforcement are a subset of all the files on the device seized.

Courts also emphasize that the requirement that law enforcement record and return to the court the calls it listens to serves to ensure law enforcement does not exceed the scope of the warrant.[156] It affords individuals the power to sue if officers have exceeded the scope.

V. POTENTIAL OBJECTIONS

A. RULE 41

On the surface, Federal Rule of Criminal Procedure 41 governing search warrants presents the biggest obstacle to my argument—but not insurmountable upon closer consideration.

First, the text of Rule 41 appears to treat the device as the thing to be seized for many purposes. Rule 41 distinguishes between tangible "property," which must be identified in the search warrant,[157] and electronically stored information. Rule 41's inventory requirement says that agents may simply list the device on the inventory,[158] rather than, presumably, individual folders or files. Thus, if officers seize a device or mirror its entire memory storage, they need only list on the inventory "one 128 GB Flashdrive" or "one Toshiba Laptop." In addition, the Rule makes clear that the 14-day limit to execute the warrant refers simply to the seizure or mirroring of the device on site, and not later searches by agents.[159]

These Rule 41 requirements, however, were not intended to answer any constitutional questions about whether the Fourth Amendment requires officers to inventory individual files and folders. The 2009 Committee Notes accompanying these amendments for electronically stored information make clear that the drafters intended the rule to remain neutral with respect to this question. The amended rule, the committee wrote, "does not speak to constitutional questions concerning warrants for electronic information" because these issues, including particularly listed file types such as a .jpg —"are presently working their way through the courts."[160]

First, and most important, the drafters said the rule left open whether a warrant must list, *ex ante*, files rather than devices with particularity as the object of the search.[161] The drafters of the rule expressly left such

156. *E.g.*, State v. Formica, 489 A.2d 1060, 1064 (Conn. App. Ct. 1985).

157. FED. R. CRIM. P. 41(a)(2)(A) (defining property as "tangible objects" such as books).

158. FED. R CRIM. P. 41(f)(1)(B) ("[T]he inventory may be limited to describing the physical storage media that were seized or copied.").

159. FED. R. CRIM. P. 41(e)(2)(B) ("The time for executing the warrant [14 days] . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.").

160. FED. R. CRIM. P. 41 advisory committee's note to 2009 amendment.

161. *Id.* ("The amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development.").

constitutional questions to case law development. They similarly wrote that the rule remains neutral with respect to whether the inventory must list specific opened or copied files.[162] Finally, it likewise says that the committee had considered setting a concrete time limit for offsite searches, but the committee decided against a nationwide standard.[163] Rather, the notes say that judges can impose particular time limits.[164]

Read with the Committee Notes, Rule 41 imposes no limit to my proposal. Although it remains neutral on the precise limits my proposal raises, it notes that these are precisely the constitutional issues that must be addressed by courts.

B. Is Opening a File a Fourth Amendment "Seizure?"

The inventory requirement normally applies only to items the police have "seized." Some scholars have argued that agents may not technically have "seized" a file under the Fourth Amendment when they open, view, or even copy it.[165] If opening or viewing a file does not count as a seizure, then one could argue officers have no obligation to list the files they open or view in an inventory. As a threshold matter, my proposal lies largely in policy, but to the extent I also rely upon the Fourth Amendment Warrant Clause, I provide below several reasons to reject the argument that opening, viewing, or copying a file is not a seizure in this context.

First, the Fourth Amendment makes a person secure in her "papers," and this term fixes the level of generality. For an inventory for ordinary property the officer must list each "effect." When we deal with digital devices, the device is of course an effect, but the files on the device are the individual's "papers." Therefore, the inventory must list each paper or each file just as it would each effect. For example, if a box contains a gun, $100 in cash, and a laptop, the police who seize the box would need to list each individual effect, especially if they open the box and take them out. On the other hand, if the police seize a car, officers need not separately list the carburetor, because it is not a separate effect.

The textual term "papers" thus tells us the level of generality to which the inventory must operate, at least if the papers are treated as papers. If the police seize a stack of letters the individual had tied up in a bundle, the officers can likely list the stack as long as they do not untie the stack and read the individual letters. That is, if the police treat the stack as an effect—merely a physical stack—listing the stack tells the individual what she needs to know to understand the nature and scope of the seizure. But opening each letter

162. *Id.* ("Current Rule 41(f)(1) does not address the question of whether the inventory should include a description of the electronically stored information contained in the media seized.").

163. *Id.* (noting unforeseen delays such as "encryption and booby traps, [or] the workload of the computer labs" militate against a nationwide time limit).

164. *Id.* ("The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued.").

165. Kerr, *supra* note 14, at 558.

treats the stack not as a single effect but rather, as a collection of individual papers.

Second, case law treats opening a file to read it as a seizure. The particularity clause has only two requirements. First, the warrant must particularly describe the "place to be searched." Second, the warrant must particularly describe the "things to be seized." As noted above, courts almost uniformly treat the device as the place to be searched and the individual files as the items to be searched for and therefore, the "things to be seized."

In *United States v. Galpin*, for example, the Second Circuit wrote that searching a device was "akin to [searching] a residence."[166] It held that simply listing the device as the thing to be seized and searched, without describing what types of files the officers intend to search for, open, and view, violates the Fourth Amendment's particularity requirement.[167] Instead, the warrant must describe the types of files the officers seek and link them to the crime for which there is probable cause.

Why must a warrant describe the types of files sought at all? Since the device is the place to be searched, the only remaining requirement is to describe the "things to be seized." If the files were not "seized," there would be no requirement under the particularity provision to describe categories of files in the warrant.

Similarly, in *United States v. Ulbricht*, the Second Circuit analogized the laptop to a home as the place to be searched, and it analogized the files within the laptop to items within a home as the things to be searched *for*[168]—i.e., the things to be seized. The court held the agents met the particularity requirement because they went beyond simply listing the laptop as the thing to be seized.[169] Instead, they listed the types of files and information they sought from the search such as "emails" concerning Silk Road or computer code concerning Silk Road.[170]

Now one might argue courts are really assessing the scope of the search and are not quite saying, as a technical matter, that officers seize a file when they open it. Kerr has argued, for example, that opening and viewing a file does not count as a new seizure beyond the initial seizure of the device.[171] But is this even true from a technical point of view?

Opening a file resembles a seizure because the officer takes control of the file in order to open it. She handles the file in some metaphorical and perhaps literal way—literally because opening a file means copying it from a hard drive or other persistent memory to the device's RAM and performing

166. United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013).

167. *Id.* at 447 (authorizing a warrant search of electronic device without limit "violated the Fourth Amendment's particularity requirement") (collecting cases).

168. United States v. Ulbricht, 858 F.3d 71, 100 (2d Cir. 2017) ("[S]earch of a computer is 'akin to [a search of] a residence[.]'" (alteration in original) (quoting *Galpin*, 720 F.3d at 446)).

169. *Id.* at 102.

170. *Id.* at 100–02.

171. Kerr, *supra* note 139, at 100.

various programming tasks on that block of memory in order to display the file on the screen.[172]

We may also consider the analogous situations of pen registers and wiretaps. The Supreme Court roughly said that a pen register "seizes" the information it obtains even though that information—each phone number dialed—is intangible under Rule 41.[173] The federal Wiretap Act requires agents to make a recording of the individual phone calls listened to and return these recordings to the court[174]—further supporting the idea that opening and viewing an individual file counts as a "seizure."

But the foregoing debate advances an overly technical understanding of the particularity provision. Neither its requirement to describe the items to be seized, nor the inventory requirement can hinge on the technical aspects of how a computer operating system opens a file and how an application program renders the file on the screen. Rather, we must preference adapting the function of the inventory over such formalism. That is, when officers search a device, open and skim a file to determine whether the file matches the file they seek, these officers are performing both a seizure and a search at the same time. The inventory requirement should be seen more broadly as requiring an accounting, in rough parlance, of the digital search. After all, we seek to further security, and an inventory can best perform this function by providing an accounting of where the officers searched. That accounting could include which folders the officers explored or which files they opened and looked at—whether we formally call that activity a Fourth Amendment "search" or "seizure."

Courts may be avoiding overly technical understandings of "seizure" and the Warrant Clause when they uniformly require officers to describe the types of files they seek when they search a digital device. Courts are imposing as a Fourth Amendment requirement such particularity under some rough combination of the search and seizure provisions of particularity.

Finally, guidance from the founding era suggests we treat opening and reading a file as a seizure for inventory purposes. After all, the Court in *Entick* made precisely that analogy, envisioning the inventory requirement applying to individual papers.[175] It pointed with particular concern to money or other bills that are paper but also valuable property, expressing a concern that the officers could simply pocket them rather than account for them in an inventory.[176] Similarly, devices contain passwords or keys to accounts, cryptocurrency, or other valuable property that officers at least have access too. If security now means what it meant then, a suspect should be told

172. *See generally* ABRAHAM SILBERSCHATZ ET AL., OPERATING SYSTEM CONCEPTS (John Wiley & Sons, Inc. 8th ed. 2009) (explaining how operating systems work).

173. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 169 (1977); *see also* Kerr, *supra* note 14, at 559–60 (arguing that this conclusion supports "the view that copying computer files should be considered a seizure").

174. 18 U.S.C. § 2518(8)(a) (2012).

175. *See supra* note 26 and accompanying text.

176. Entick v. Carrington, 19 Howell's St. Tr. 1029, 1064–65 (CP 1765).

whether officers accessed these valuable passwords or keys, and particularly, the underlying accounts.

C. *BEYOND "FILES"*

For much of this paper I have used the term "file" as synonymous with the thing to be seized. That is, in a very rough way, I treated a computer file as the appropriate level of specificity for the particularity requirement—as do courts and scholars generally. But computers use and create files in ways that might differ significantly from how we, as users, conceptualize the gathered data.

On the one hand, our treatment and that of a computer sometimes coincide. An image file of a photograph corresponds to our notion of a physical photograph. In both cases, the thing to be seized is essentially a photograph, though of course the file of the photograph contains metadata instructing the program how to open the file, and the pixels themselves can be coded in various ways. Nevertheless, the mapping is so close that a person could look at the pattern of the underlying bytes and probably make out an image.

On the other hand, computers will often create large files composed of what we in the ordinary world would consider individual items. These types of files challenge my earlier equating of files with the item to be seized (and described in the inventory). For example, many desktop email programs such as Outlook create massive files containing all of a person's emails, contacts, and other information in a certain folder—a .pst file. Devices will also create a single file containing a thumbnail image of each file for quicker loading into a file directory such as Finder on Macs—sometimes called a thumbnail.db file.

The same principle, and problem, will apply to metadata stored on the device in the form of files or databases, but in such aggregate that treating the file as the relevant item will not work. A device might store location data in many different ways, distributed or aggregated.

We will not want to treat these aggregated file-databases as single files because they contain far more information than the chunks into which we customarily aggregate information. Instead, we must develop a framework for narrowing the scope of these files. For example, we can treat individual emails as the relevant item to be seized, because emails resemble letters and are often standalone. On the other hand, for text messages, we will likely need to treat an entire conversation as the relevant unit of particularity.

In either case, how we aggregate the information in our minds usually corresponds with how the graphical interface of the relevant application aggregates the information. A text program will group together messages with a particular person or a group of persons, and we think of these as conversations. Now we may seek to limit the timeframe so that officers cannot search the conversation between two people going back years, but imposing this limit is a relatively easy task using the native software.

Similarly, even though a device may contain a single file with *all* the thumbnails of *all* the other files, we cannot treat this thumbnail database as a single file or we would, in effect, simply afford agents access to the entire

device again. Instead, we must restrict searches to follow the path of the native software so that officers will view thumbnails only in folders they are otherwise permitted to search. In addition, officers will need to list in the inventory the folders they viewed and whether those folders disclosed thumbnails.

In some cases, we can insist that officers simply turn off any thumbnail feature to limit broad, exploratory searches, allowing thumbnail views for folders or filetypes within the warrant's scope. This limit will again require that officers have a reason to open a particular file or type of file.

We will want to treat metadata in a similar, commonsense way rooted in how the user and the native software treats, organizes, and aggregates the information, and how we treat the information in the real world. For example, if agents want to seek location data on a device, the warrant will need to authorize a search for location data expressly, and limit then its scope by time or location. If officers are investigating a particular robbery, then the limit will likely be a few days or hours. With this limit in hand, the forensic software will direct officers to precisely those files in those apps that store location data and cull the location for that time period from whatever underlying source, file or database.

D. CHAIN OF CUSTODY AND FORENSIC BEST PRACTICES

In addition to an inventory, I have proposed that law enforcement return to the defendant and destroy any copies of files it does not need. If the police have searched an entire device and have identified and copied ten files, it must destroy the rest, numbering perhaps in the thousands. This proposal runs into some serious practical objections that I address below.

First, for chain of custody and other evidentiary forensic purposes, law enforcement best practices require forensic examiners to mirror and keep a copy of an entire device's memory to prove, at trial, that a particular file truly came from that device.[177] Second, law enforcement may not be able to find all the incriminating information on a device within the time frame, but do not want to trust the suspect or defendant not to destroy the returned data. Third, law enforcement may develop new facts independently that allow them to re-search the data for other crimes (based upon a new warrant).

We can address these problems in a number of ways. First, as to authenticating files, we can give the defendant the option to stipulate that a given file came from a given device. This stipulation means the prosecution will not need to otherwise authenticate a particular file as having come from the device, and they will not need to keep a mirror of the entire device.

Second, it is true that during a longer investigation, law enforcement will need to have future access to the entire media to search again, perhaps with a new warrant. We can solve this problem by storing a mirror image of the entire media with a neutral third party such as the court. This solution is not ideal, of course. A person still feels insecure that his entire digital life remains in the hands of others. Nevertheless, if we can create a true vault, this seems a

177. *See, e.g.*, United States v. Ganias, 824 F.3d 199, 215 (2d Cir. 2016).

sensible middle ground for mitigating a suspect's concerns and ensuring law enforcement's needs.

E. THE EXCLUSIONARY RULE

One might object that an inventory requirement will afford criminal defendants yet another ground to suppress evidence. Defendants will argue a court must suppress some or all evidence gleaned from any search in which officers have failed to provide an inventory at all, provide one in a timely fashion, or provide a complete one.

My response is simple: A failure by law enforcement to create or provide an inventory for electronic files should generally not result in suppression of evidence. After all, a person subject to search has a ready and immediate remedy to the failure by police to provide an inventory—a court can order the police to provide one. Indeed, before it even comes to such a request, courts can routinely require officers to create an inventory as part of any return on the warrant. The court can hold in contempt officers who fail to provide the inventory or show good cause why they have not done so.[178] In filed cases, courts can order an inventory as part of discovery.[179]

The rule here may differ from that in the physical world. When police enter a home to search, the requirements that the police show the person the warrant and inventory the items taken assures the suspect that the entry is lawful, that the scope of the searched undertaken is authorized, that the police are entitled under the warrant to take the items on the inventory, and finally, that they have a receipt of the items taken to guard against theft.

In the electronic world, the police likely search the device outside the presence of the suspect, who can satisfy herself that the police abided by the terms of the warrant only after the search. As a result, a late inventory merely delays when she may compare the inventory with the scope of the warrant —rendering unnecessary the suppression of evidence as a remedy. And again, courts can remedy these delays before they happen, or afterwards with contempt orders.

Finally, current Supreme Court precedent would likely decline to apply a suppression remedy to most failures to provide an inventory. For example, in *Hudson v. Michigan*,[180] the Court held that even a deliberate failure of the police to knock and announce in executing a search warrant on a home would not result in exclusion of the evidence found within. The rationale was largely one of causation—even if the police had knocked and announced, they would still have entered the premises and obtained the evidence. Applying that principle here, we can see that the failure of the police to provide an inventory

178. United States v. Gross, 137 F. Supp. 244, 249 (S.D.N.Y. 1956) (ordering the government to prepare inventory or face suppression of evidence).

179. United States v. Zovluck, 274 F. Supp. 385, 391 (S.D.N.Y. 1967) (ordering the government to prepare an inventory of items seized under discovery provisions); *cf.* FED. R. CRIM. P. 16(a)(1)(E) (describing government's obligations to a defendant that requests access to materials "within the government's possession, custody, or control").

180. Hudson v. Michigan, 547 U.S. 586, 594 (2006).

should not lead to suppression because, even if agents had provided an inventory, they still would have obtained and viewed the same evidence.

By contrast, if law enforcement violates the other of my proposals—the requirement to return property in a timely fashion—a court should suppress any evidence the police found from searching the media after they should have returned it. In that case, the police *do* obtain evidence they would not have had they returned the property.

F. FILING AN INVENTORY WITH THE COURT: PRIVACY

Rule 41 requires the inventory to be filed with the clerk of the court. This procedure would potentially make very detailed inventories available to the public and the press. My proposal would potentially invade the privacy of suspects more than protect it—at least if these inventories remained open to the public.

The potentially public nature of inventories presents serious challenges, both to my proposal and to courts in general. I would therefore add the following: First, suspects or defendants should be given the opportunity to waive a detailed inventory or waive the *filing* of a detailed inventory with the clerk of the court. Instead, individuals would retain the right to receive a copy of the detailed inventory without fear that it would be publicly filed.

In the alternative, the court could still receive and file inventories but under seal. These inventories would remain under seal in the ordinary case, to protect the grand jury process as well as the privacy of the individual and any third parties whose data might be included in the device. Courts currently refuse to unseal such inventories, even for the media in prominent cases.[181]

VI. THE FOUNDING GENERATION'S VIEW ON WARRANTS AND INVENTORIES

This Part first argues that the Fourth Amendment as originally understood included an inventory and return requirement for seized physical things. Second, it shows that this requirement did not apply directly to papers because the founding generation likely banned the search and seizure of papers in criminal cases. Some of those same sources suggest that *were they* to allow paper searches, they would have required officers to inventory the papers seized. I urge that course—to impose a complete ban on paper searches would impose too rigorous an originalist perspective. Finally, I address contrary case law holding that the Fourth Amendment does not require an inventory.

But why originalism at all? First, the problems the founding generation faced with respect to paper searches parallel those today, and led the framers to craft the state and federal search and seizure provisions in the first place. Second, originalism plays a central role in the Supreme Court's current Fourth Amendment jurisprudence. Third, originalism refocuses the Fourth Amendment inquiry from the Reasonableness Clause to the Warrant Clause,

181. United States v. Sealed Search Warrants, No. 99-1096, 1999 WL 1455215, at *8 (D.N.J. Sept. 2, 1999).

and from a conception of privacy-solely-as-secrecy to a conception that includes a more robust vision of what it means to be "secure" under the Fourth Amendment.

That is, over the last 50 years, the Supreme Court and scholars have focused tremendous attention to what counts as a Fourth Amendment "search"—what type, for example, of electronic surveillance even counts as a search triggering the Fourth Amendment Warrant Clause. The Court in *Riley v. California*, for example, determined whether a warrant was necessary for a search of an electronic device and announced, proudly, that officers must "get a warrant."[182] The Court did not spend any time discussing how those warrants should be executed.

But for the founders, the Warrant Clause was likely the key to the Fourth Amendment. In the view of one leading scholar, Thomas Y. Davies, the Warrant Clause was the only "operative" portion of the Fourth Amendment.[183] He focuses primarily on issuing the warrant, and the important role magistrates played in ensuring customs officials, or constables, did not engage in unsupervised, broad searches. But for our purposes, a renewed focus on the Warrant Clause brings with it a focus on the inventory requirement.

A. DOES THE CONSTITUTION REQUIRE AN INVENTORY AND RETURN?

I argue in this Section that the Fourth Amendment as originally understood requires an inventory and return for physical things based upon its (i) history, (ii) long, uninterrupted practice, (iii) the text, and (iv) some recent case law. Many of these reasons as applied to ordinary property likewise suggest that the Fourth Amendment requires an inventory for individual electronic files.

First, in assessing its history, the Court has pointed to the founding era as particularly salient in interpreting the Fourth Amendment. Often it relies upon a very specific founding era practice such as in *United States v. Watson*.[184] At other times, it points to the principles animating the Fourth Amendment as guidance.[185] Even in the most contemporary, electronic context such as the Court's recent case, *Carpenter v. United States*, the Court repeatedly pointed to founding era principles that animate the Fourth Amendment.[186]

Moreover, the Court has not hesitated to rely directly upon the framing era practices concerning the procedures attending the granting or execution of a warrant—even when reading in requirements not contained in the text. For example, the Warrant Clause contains no requirement that officers knock

182. Riley v. California, 573 U.S. 373, 403 (2014).

183. Davies, *supra* note 6, at 551 ("[T]he Framers clearly understood the warrant standards to be the operative content of the Fourth Amendment.").

184. United States v. Watson, 423 U.S. 411, 418 (1976).

185. *Riley*, 573 U.S. at 403 (2014) ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."); Georgia v. Randolph, 547 U.S. 103, 143 (2006) (Scalia, J., dissenting) (discussing the "common-law trespass" origins of the Fourth Amendment).

186. Carpenter v. United States, 138 S. Ct. 2206, 2238–40 (2018).

and announce before entering a home, but in *Wilson v. Arkansas*, the Court held that the Fourth Amendment Reasonableness Clause requires officers to "knock and announce" when executing a search warrant for a home.[187] The Court relied almost entirely upon the founding era common law, which required officers executing warrants to knock and announce.[188]

In particular, the Court pointed to English and American case law, treatises, and statutes.[189] It cited leading English treatises on English common law, including those of William Blackstone,[190] Matthew Hale,[191] and William Hawkins,[192] for the knock and announce rule, as well as leading English cases such as *Semayne's Case*.[193] It showed how American colonies adopted wholesale the common law of England in their reception statutes,[194] and cited state supreme court cases from the early-nineteenth century recognizing the knock-and-announce rule.[195]

As for the inventory, we have already noted that one of the key cases leading to the Fourth Amendment, *Entick*, pointed to the lack of an inventory and return as a reason to find the seizure of papers there invalid.[196] Moreover, James Otis, in his argument in what is commonly called the *Writs of Assistance Case* in Boston in 1761, placed particular reliance on the open-ended nature of those writs.[197] They permitted not only general searches, but were permanent, that is, were not returned to a court. In Otis' view, and John Adams' as well, for a writ to be valid, the officer "must return it."[198] Moreover, Otis said the reason for requiring a return was to keep the officer accountable—evidently for the scope, legality, and duration of the search.[199] Thomas Clancy has ranked the return requirement as one of the key concerns of the founding era in formulating the Fourth Amendment, along with the requirement of an oath upon probable cause.[200]

Statutes near the time of the framing similarly advanced scrupulous adherence to the inventory or return requirement for searches in criminal

---

187. Wilson v. Arkansas, 514 U.S. 927, 934, 936 (1995).

188. *Id.* at 931–34.

189. *Id.* at 931–36.

190. *Id.* at 933 (citing 3 WILLIAM BLACKSTONE, COMMENTARIES *412).

191. *Id.* at 932 (citing 1 MATTHEW HALE, THE HISTORY OF THE PLEAS OF THE CROWN *582).

192. *Id.* (citing 2 WILLIAM HAWKINS, A TREATISE OF THE PLEAS OF THE CROWN 138 (Thomas Leach ed., 6th ed. 1787)).

193. *Id.* at 931 (citing Semayne's Case (1604) 77 Eng. Rep. 194, 195; 5 Co. Rep. 91a, 91b).

194. *Wilson*, 514 U.S. at 933 (citing, for example, the Virginia reception statute: "[T]he common law of England . . . shall be the rule of decision, and shall be considered as in full force, until the same shall be altered by the legislative power of this colony" (alterations in original)).

195. *Id.* (citing, for example, Howe v. Butterfield, 58 Mass. (1 Cush.) 302, 305 (1849)).

196. Entick v. Carrington, 19 Howell's St. Tr. 1029, 1067 (CP 1765).

197. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 992, 997 (2011).

198. *Id.* at 997 ("If an officer will justify under a Writ he must return it." (quoting John Adams' notes of Otis' argument)).

199. *Id.* at 1000 (without the return, "[a] man is accountable to no person for his doings").

200. *Id.* at 1056–58.

cases.[201] For example, a Pennsylvania statute enacted in 1791 required an inventory for things seized in cases of burglary, robbery, and larceny.[202] In 1804, Massachusetts enacted a statute requiring an inventory for stolen goods seized by officers executing arrest warrants for larceny: The officer executing the warrant had to create "a true inventory or schedule [to] be made in or annexed to the return."[203]

In the 1770s and 1780s, several states passed laws prohibiting trading with the enemy and authorized warrants to search for and seize contraband. These laws required any officer executing a warrant to list by inventory (and often apprize) the things seized, including Connecticut[204] and New York.[205] New York's 1781 law, for example, contains many of the same requirements as today's Rule 41: an inventory, with another witness, delivered to the issuing judge.[206] In particular, it required that "the constable shall under the inspection of the two freeholders he shall have taken to his assistance, make an inventory of the goods so seized and deliver the same with the said bond to the justice . . . ."[207]

Founding era practice also confirms these requirements. The requirements for search warrants appear almost entirely in the context of search warrants for stolen goods. In the founding era, justices of the peace were the primary officials who issued search warrants in ordinary criminal cases for stolen goods.[208] Indeed, justices of the peace oversaw most of the initial phases of criminal cases, issuing both arrest warrants and search warrants to constables, who were required to return these warrants either to the justice of the peace who issued it, or another justice of the peace.

Justices of the peace were often lay persons, albeit from the upper echelons of society, who may not have been trained lawyers.[209] As a result, they

201. 2 THE REVISED STATUTES OF THE STATE OF NEW YORK, pt. IV, ch. 2, tit. 7, art. 3, § 26, at 746 (Albany, Packard & Van Benthuysen 1829) (requiring officers "to bring such property before the magistrate issuing the warrant"); An Act for the More Easy Discovery and Effectual Punishment of Buyers and Receivers of Stolen Goods 1782, 22 Geo. III c. 58, §§ 2–3 (Eng.).

202. 1791 Pa. Laws 120–21 ("[T]he said magistrate shall forthwith cause an inventory to be taken of the said goods, and shall file the same with the Clerk of that court in which the accused person is intended to be prosecuted . . . .").

203. Act of March 16, 1805, ch. 143, § 15, 1804 Mass. Acts 245.

204. An Act in Further Addition to and in Alteration of the Act Entitled An Act More Effectually to Prevent Illicit Trade, 1780 Conn. Pub. Acts 15.

205. Act of April 13, 1782, ch. 39, § 5, 1782 N.Y. Laws 479 (attempting to "more effectually prevent illicit trade with the enemy").

206. *Id.*

207. *Id.*

208. Fabio Arcila, Jr., *In the Trenches: Searches and the Misunderstood Common-Law History of Suspicion and Probable Cause*, 10 U. PA. J. CONST. L. 1, 6 (2007); *cf.* 2 WILLIAM BLACKSTONE, COMMENTARIES *290 (noting that arrest warrants were issued "ordinarily by justices of the peace").

209. JOHN H. LANGBEIN, THE ORIGINS OF ADVERSARY CRIMINAL TRIAL 46 (A.W. Brian Simpson ed., 2005) ("The JPs were mostly local gentlemen . . . . [D]rawn from the higher social orders . . . . They were seldom lawyers, seldom legally trained.").

relied upon justice of the peace manuals. These manuals have served as an important source for determining early criminal law practice.[210]

Many of the founders would have been very familiar with these manuals. Thomas Jefferson served as a Justice of the Peace (hereinafter JP), as did his father, and his library held many of these manuals.[211] George Washington served as a JP for 14 years, as did his father, his grandfather, and his great-grandfather.[212] Ben Franklin published a leading JP Manual, *The Conductor Generalis*, in 1749.[213] James Madison, the prime author of the Fourth Amendment, subscribed to the leading JP manual in Virginia.[214]

These justice of the peace manuals confirm that the founding era practice uniformly required a return on warrants. In the case of search warrants, the manuals expressly require constables who seize items to bring them to a court to determine whether they were in fact stolen.[215] These manuals do not appear to require a written inventory—but the immediate return to court of the items themselves served precisely the same function. Nearly every American justice of the peace manual relies upon Lord Hale's treatise in expressly requiring a return for an accounting of the goods. William Hening's Virginia manual typically formulates this requirement: The warrant "ought to command that the goods found together with the party in whose custody they are found, be brought before some justice of the peace" to determine whether they are stolen.[216] Case law close to the founding era also imposes these requirements.[217]

---

210. *See generally* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791 (2009) (citing to justice of the peace manuals to discuss early Fourth Amendment history).

211. 2 Catalogue of the Library of Thomas Jefferson 303–04 (E. Millicent Sowerby ed., 1953).

212. DOUGLAS SOUTHALL FREEMAN, GEORGE WASHINGTON 34 (1948); Henry Graff & Allan Nevins, *George Washington: President of the United States: Marriage and Plantation Life*, BRITANNICA (Mar. 11, 2020), https://www.britannica.com/biography/George-Washington/Marriage-and-plantation-life [https://perma.cc/LQM6-CUQH].

213. Larry M. Boyer, *The Justice of the Peace in England and America from 1506 to 1776: A Bibliographic History*, 34 Q.J. LIB. CONGRESS 315, 323 (1977).

214. WILLIAM WALLER HENING, THE NEW VIRGINIA JUSTICE (1795) (listing "Subscriber's Names").

215. *Id.* at 403; *see* 2 MATTHEW HALE, THE HISTORY OF THE PLEAS OF THE CROWN 150 (1847); *see also* JOSEPH GREENLEAF, ABRIDGMENT OF BURN'S JUSTICE OF THE PEACE AND PARISH OFFICER 324 (1773) (explaining that upon return, the justice of the peace is to determine whether the goods were stolen); JAMES PARKER, THE CONDUCTOR GENERALIS: OR, THE OFFICE, DUTY AND AUTHORITY OF JUSTICES OF THE PEACE, HIGH-SHERIFFS, UNDER-SHERIFFS, CORONERS, CONSTABLES, GAOLERS, JURY-MEN, AND OVERSEERS OF THE POOR 386 (Phila. 1801).

216. HENING, *supra* note 214, at 403.

217. Grumon v. Raymond, 1 Conn. 40, 45–46 (1814); Bell v. Clapp, 10 Johns. 263, 265 (N.Y. Sup. Ct. 1813).

Second, since then, cases[218] have reflected and statutes[219] have required an inventory or return in an apparently uninterrupted continuum.[220] Indeed, Rule 41 traces its roots to a 1917 New York statute,[221] that in turn likely rests upon principles codified in New York at least by 1829.[222] Today federal and state statutes alike require that officers return warrants and prepare inventories.[223]

Many might resist a reflexive reliance on original practice or understanding in construing the Fourth Amendment. But in this case, the original practice provides a surprisingly unambiguous picture of the central role the return played in England and the colonies, both as ordinary practice and as important rhetoric leading to the Fourth Amendment. The concerns animating the framers remain the same today: accountability, rule of law, and judicial oversight. Indeed, since the founding, states have apparently required a return and inventory continuously and pervasively up until the present. As noted above, today, nearly every state requires an inventory and return.[224]

Outside the context of search warrants, many in the founding era would have been quite familiar with inventories touching many aspects of their lives and deaths. Colonists used detailed inventories widely, including probate inventories to list things in the estate upon death;[225] inventories listing

218. Shannon v. Spencer, 1 Blackf. 526, 529 (Ind. 1822); Banks v. Farwell, 38 Mass. 156, 157 (1838); Williams v. Sheppard, 13 N.J.L. 76, 81 (1832); Green v. Rumsey, 2 Wend. 611 (N.Y. Sup. Ct. 1829); Cabiness v. Martin, 14 N.C. 454, 456 (1832); Watt v. Greenlee, 7 N.C. 246, 246 (1819); Hussey v. Davis, 58 N.H. 317, 317 (1878); *see also* THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 305 (1868) (citing cases).

219. 18 U.S.C. § 3115 (1948); 18 U.S.C. §§ 622–27 (1925) (requiring written inventory); Espionage Act of 1917, Pub. L. No. 65-24, c. 30, Title XI, §§ 12–17, 40 Stat. 217, 229–30 (1917) (same); Act of April 20, 1855, ch. 215, § 25, 1855 Mass. Acts 635; 2 THE REVISED STATUTES OF THE STATE OF NEW YORK, pt. IV, ch. 2, tit. 7, art. 3, § 26, at 746 (Albany, Packard & Van Benthuysen 1829) (requiring officers "to bring such property before the magistrate issuing the warrant").

220. These sources address searches for criminal investigations. The same principles and requirements do not always hold for searches for more administrative purposes, such as to remedy health concerns or even to find goods upon which a duty had not been paid. For example, the Collection Act of 1789 authorized federal officers to obtain warrants to search homes, stores and other places for goods upon which a duty had not been paid. The provision does not require an inventory or even a return; instead, the federal officer himself must hold the goods until trial. The Court has long struggled with the status of so-called administrative searches; for our purposes, we may put to the side these searches since they do not fall within the central realm of criminal investigations while still acknowledging the difficult line-drawing such a sidelining entails.

221. N.Y. CODE CRIM. PROC. 805 (1917) ("The officer must forthwith return the warrant to the magistrate, and deliver to him a written inventory of the property taken.").

222. 65 CONG. REC. 3307 (1917) ("The new title as presented by the conferees was based upon the New York law on this subject and follows generally the policy of that law.").

223. FED. R. CRIM. P. 41; N.C. GEN. STAT. § 15A-257 (2017); NEB. REV. STAT. ANN. § 29-816 (West 2015); VA. CODE ANN. § 19.2-57 (2015); FLA. STAT. ANN. § 933.12 (LexisNexis 2011); OHIO R. CRIM. P. 41(D)(1); PA. R. CRIM. P. 209.

224. *See supra* note 223.

225. *E.g.*, An Act Directing the Manner of Granting Probats of Wills, and Administration of Intestates Estates, ch. 2, § 15, 1749 Va. St. 21 (requiring executors to prepare a "true and perfect inventory" of the decedent's possession and return the inventory to the court); Act of Jan. 27,

enslaved persons; inventories listing things from a debtor seized or to be sold;[226] and in the early republic, inventories to list goods for taxation or duties—including ship manifests and detailed records of goods and liquor entering the country, their weight, or their proof.[227] The colonists used inventories to keep accounts and protect the value of property, and it should be no different when it comes to officers seizing private property pursuant to a warrant.

Third, the text of the Fourth Amendment affords an indirect avenue to support an inventory requirement. The text requires the warrant to list, with particularity, the things to be seized. The inventory lists the things actually seized. When the officer returns the inventory (or the goods themselves) to the magistrate, the magistrate of course must determine whether the things seized match the items originally listed in the warrant—at least by type.

The inventory thus enforces the particularity requirement upon the return. In the founding era, a magistrate would examine the goods seized to determine whether they were, in fact, stolen.[228] Since that time[229] to today, the inventory allows the magistrate upon return—or the suspect—to ensure the officers acted within the scope of the warrant by comparing the inventory with the items listed in the warrant.[230] The warrant and inventory were used as evidence in any subsequent lawsuit for trespass or a criminal larceny case against the officer or individual party who may have falsely obtained the warrant.[231]

For example, in 1814 in *Grumon v. Raymond*, a person claimed someone stole two bags, worth $1, which were stamped "A. C." and "M. M."[232] A JP issued a warrant ordering a constable to search the suspected place and return anything he found to the justice at his home.[233] The constable found bags, though not quite meeting the description in the warrant: *two* bags marked "M.

1749, ch. 381, § 3, 1974 Pa. Laws 96 (providing that a ship commander shall create a "true and perfect inventory" of the possessions of any passenger who dies on the ship).

226. An Act for the Better Enabling of Creditors to Recover Their Just Debts from Persons who Abscond Themselves, ch. 101, § 1, 1752 N.J. Laws 395.

227. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29 (1789).

228. Bell v. Clapp, 10 Johns. 263, 265 (N.Y. Sup. Ct. 1813); *see* Grumon v. Raymond, 1 Conn. 40, 43 (1814); HALE, *supra* note 215, at 150; HENING, *supra* note 214, at 403.

229. N.Y. CODE CRIM. PROC. § 809 (1917) (requiring magistrate to return the property if it does not match that originally described in the warrant); State v. Hall, 16 A. 329, 329 (Me. 1888).

230. United States v. Birrell, 269 F. Supp. 716, 721 (S.D.N.Y. 1967) ("The ostensible purpose of the inventory requirement, suggested by this statutory scheme, is to enable the Court to determine—on the face of the warrant, return and inventory—whether the seizure was properly limited to the property identified in the warrant."); *cf.* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *22 (D. Or. June 24, 2014) ("The warrant and an inventory of seized property are returned to the issuing judge under Rule 41, and there are provisions to convey this information to the person whose property was seized."), *aff'd*, 843 F.3d 420 (9th Cir. 2016).

231. Stone v. Dana, 46 Mass. 98, 104, 108–10 (1842); 5 THE ENCYCLOPÆDIA OF EVIDENCE 734 (Edgar W. Camp & John F. Crowe eds., 1905) ("The defendant may offer in justification the affidavit and original warrant, or the complaint on which the warrant was issued.").

232. *Grumon*, 1 Conn. at 40.

233. *Id.* at 40–41.

M.," and another marked not "A. C.," but "A. G."[234] He nevertheless seized these, arrested the occupants, and brought the bags and suspects to the justice.[235]

The justice ruled that the evidence was insufficient.[236] The case report does not tell us why—it appears the justice found the bags seized did not sufficiently match the description of the bags from the complainant. This case thus appears to illustrate precisely the matching function I sketched above: The return, here serving the function of an inventory, allowed the issuing justice to ensure the constable had acted within the scope of the warrant and had met the express requirements of *particularity*. Here, the warrant authorized the constable to seize a bag marked, "A. C." but he instead seized one marked "A. G."—violating the express terms of the warrant.[237]

Today, in the physical world, the inventory works similarly.[238] Even if the warrant describes the items to be seized more generally, such as drug making equipment, the inventory will list the specifics seized, such as a pill making machine. If the suspect seeks to get the machine back, the judge can determine whether the machine matches the description—drug making machinery—or is in reality a sewing machine, for example. Of course, officers may seize contraband not listed in a warrant under the plain view doctrine, though here too they must list those items on an inventory.

We can see this dual role the magistrate plays—issuing the warrant and examining the items seized pursuant to it—as an inextricably linked symmetry. The purpose of the Warrant Clause is to impose a neutral magistrate between zealous law enforcement and suspect,[239] to ensure through the particularity clause that the magistrate, not the officer, determine what shall be seized. The warrant must describe it with particularity to leave the officer little discretion in what to seize, and what not to seize;[240] the officer, in theory, need only compare the item with the description in the warrant. The inventory, the return, and the magistrate's own comparison of the warrant with the item seized merely continues this critical function of

234. *Id.* at 41.

235. *Id.*

236. *Id.*

237. In the end, the defendants, the constable and the justice of the peace, were found liable for a separate reason: The warrant was an unlawful general warrant because it authorized a search not only in the suspected home, but in any home in the town whatsoever. *Id.* at 43.

238. FED. R. CRIM. P. 41(f)(1)(B) ("*Inventory.* An officer present during the execution of the warrant must prepare and verify an inventory of any property seized."); FED. R. CRIM. P. 41(f)(1)(D) ("*Return.* The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant.").

239. Johnson v. United States, 333 U.S. 10, 14 (1948) (stating that probable cause is to be determined "by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime").

240. Marron v. United States, 275 U.S. 192, 196 (1927) ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

interposing the magistrate's neutral judgment; it is part of the particularity requirement as well as an enforcement of it.[241]

On the other hand, what historically was an important matching function has become far more theoretical; today, magistrate judges must receive the inventory, but in practice are unlikely to review it to ensure the items seized fit under the original warrant. Instead, Rule 41 and practice largely deputize, metaphorically, suspects or defendants to perform any reviewing function to ensure the search fell within the limits of the warrant. But this shift should not matter for our purposes. The inventory performs the same function, and under my proposal, it will largely be the suspect or defendant who ends up obtaining and reviewing the inventory of the files officers actually view.

Finally, recent case law strongly implies that the Fourth Amendment requires an inventory and return. Now *Groh* did not expressly assert that the Fourth Amendment requires an inventory and return. But it held that the warrant must list the items to be seized, not simply the affidavit, so to assure the person searched that the search comports with the scope of the warrant; for electronic searches conducted afterward offsite, the inventory becomes the only means an individual can conduct this comparison.

In *United States v. Berger*, the Supreme Court held that the wiretapping law there violated the Fourth Amendment. As in *Entick*, the Court emphasized that the New York wiretapping law struck down failed to require officers create an inventory of each conversation they seized.[242] The Court has also held that the Due Process Clause requires officers provide suspects at least some notice that they have taken their property. The Court suggests this notice must include an inventory.[243]

B. PAPERS IN THE FOUNDING ERA

But the founding generation likely would not have applied their insistence on an inventory to papers because they likely banned such searches and seizures entirely. This Section shows why. Indeed, the founding generation faced many of the same problems with regard to searches of papers as we do with electronic devices, particularly the problem of searching for one guilty paper in a pile of innocent ones. But at least some of those same sources suggest that *were they* to approve searches and seizures of papers, they would have required an inventory and return. This Section argues that since it would go too far to read the Fourth Amendment as banning paper searches

241. *Cf. id.* at 196 (seeming to treat the return and matching function as part of Congress' effort to further the particularity requirement of the Warrant Clause).

242. Berger v. New York, 388 U.S. 41, 57 (1967). The Court contrasted New York's law with one that would satisfy Fourth Amendment requirements by noting about that other law: "Finally the officer was required to and did make a return on the order showing how it was executed and what was seized." *Id.*

243. City of W. Covina v. Perkins, 525 U.S. 234, 240 (1999) (discussing an instance in which the officers provided "an inventory of the property taken. . . . [W]e need not decide how detailed the notice of the seizure must be . . . .").

and seizures entirely, we should take up the inventory as the appropriate, still originalist-in-this-sense, solution.

1. *Wilkes* and *Entick* Cases

The prominent English cases leading to the Fourth Amendment protections for papers concerned two English publishers subjected to law enforcement scrutiny for their writings and publications. The Crown considered their critiques of the government to be seditious libel.[244] The government sent officers to conduct very broad searches of one suspect, John Wilkes, a publisher, writer, poet, and a member of parliament.[245]

The scale of the search reminds us of the similarity to today's electronic devices. The King's messengers seized or searched an equally wide variety of papers: books, personal letters, drawings, poems, parliamentary papers, legal documents, financial documents, and nearly any other document an educated and prolific reader and writer such as Wilkes would have.

In *Entick v. Carrington*, John Entick, another writer suspected of authoring another set of anonymous pamphlets critical of the Crown, i.e., sedition libels, suffered a similarly exhaustive search.[246] In this case, the warrant did name him, but the messengers seized hundreds of documents.[247]

Beyond these court decisions, many other sources show that the founding generation, and their English counterparts, protected their home cache of papers with the same jealousy as we protect the privacy of our smartphones. One pamphlet catalogued some of the possibilities: "The merchant has his secrets of trade; the philosopher his discoveries in science. . . . Many have their Wills, settlements, and dispositions of their estates, sealed up in silence not to be broke . . . ."[248]

Another pamphlet similarly foreshadows the many court avowals concerning the deep privacy contained by our electronic devices:

> Papers . . . are our closest confidents; the most intimate companions of our bosom; and next to the recesses of our own breasts, they are the most hidden repository we can have. Our honour and fame, our estates, our amusements, our enjoyments, our friendships, *are*, and even our vices *may be*, there: things that men trust none with, but themselves; things upon which the peace and quiet of families, the

244. CUDDIHY, *supra* note 210, at 440; Donohue, *The Original Fourth Amendment*, *supra* note 6, at 1201.

245. Wilkes v. Wood (1763) 98 Eng. Rep. 489, 498–99 (KB).

246. Entick v. Carrington, 19 Howell's St. Tr. 1029, 1030–31 (CP 1765).

247. *Id.* at 1030 (describing seizure of "100 printed charts, 100 printed pamphlets &c. &c.").

248. Schnapper, *supra* note 6, at 889 (quoting A Letter to the Right Honourable the Earls of Egremont and Halifax, His Majesty's Principal Secretaries of State, on the Seizure of Papers 8 (London 1763)) (emphasis omitted).

> love and union of relations, the preservation and value of friends, depend.[249]

Even a modern phenomenon such as collecting a defendant's cellphone location data has its parallel in the founding era. John Wilkes' diaries contain a daily accounting of where he dined, and with whom.[250] In the 1770s, at least, he dined out nearly every night.[251] George Washington famously kept numerous types of diaries, including a daily diary of farming events at Mt. Vernon.[252] He did not dine out as often as Mr. Wilkes.

Conceptually, these early privacy advocates identified the same problems we face today with paper searches. They emphasized what Donald A. Dripps has called the "pooling problem": A search for concededly guilty papers, or contraband papers, will inevitably sweep up an entirety of innocent, private papers.[253]

In addition, these founding era privacy advocates also worried about government fishing expeditions. Father of Candor—a pamphleteer sometimes identified as Judge Pratt from the *Entick* case—wrote that the government, upon the barest suspicion, might search all a person's documents until he finds evidence of guilt.[254] "It is a fishing for evidence."[255] He called the practice "the worst sort of inquisitions," violating "every private right."[256] This fishing expedition finds a modern analogue: Agents often retain a person's device to perform, years later, additional searches for new crimes.[257]

Up until 1967, courts in the United States imposed a similar law. In cases such as *Boyd v. United States*[258] in 1886 and *Gouled v. United States*[259] in 1921, the Supreme Court adhered somewhat firmly to the rule against seizing

---

249. *Id.* at 890 (alteration in original) (quoting A LETTER TO THE RIGHT HONOURABLE THE EARLS OF EGREMONT AND HALIFAX, HIS MAJESTY'S PRINCIPAL SECRETARIES OF STATE, ON THE SEIZURE OF PAPERS 8–9 (London 1763)).

250. WILKES, *supra* note 4, at 4. For example, on August 1, 1770, Wilkes "attended Mr Horne's trial at Guildford, dined at Serjeant Glynn's lodgings with the Serjeant, Horne, Reynolds, R. Oliver, Missing &c. in the evening passed thro' Epsom to Croydon, lay at the George there." *Id.* at 9.

251. *Id.* In 1772, July 2: Mr. Wilkes dined "at Mr Jacob's, Druggist[.]" *Id.* at 54. July 3: Mr. Wilkes "dined at the London Tavern." *Id.* July 4: Mr. Wilkes "dined in Prince's Court." *Id.* July 5: Mr. Wilkes dined "at Mr Stavely's in Friday Street." *Id.* July 6: Mr. Wilkes "dined at the Mermaid in Hackney." *Id.* at 54.

252. 1 THE DIARIES OF GEORGE WASHINGTON 211–66, 1748–65 (Donald Jackson & Dorothy Twohig eds., 1976) (showing diary entries from January 1 to April 11, 1760).

253. Dripps, *supra* note 6, at 51, 101.

254. Letter from Candor to the Public Advertiser 31 (2d ed. 1764).

255. *Id.*

256. *Id.*

257. *See* United States v. Ganias, 824 F.3d 199, 200 (2d Cir. 2016); United States v. Wey, 256 F. Supp. 3d 355, 361–63 (S.D.N.Y. 2017).

258. Boyd v. United States, 116 U.S. 616, 629–30 (1886).

259. Gouled v. United States, 255 U.S. 298, 309 (1921).

papers to further a criminal investigation—at least when those papers were merely evidence of a crime not themselves instrumentalities of the crime.[260]

2. A Ban on Paper Searches?

Numerous scholars have concluded that the Fourth Amendment as originally understood prohibited the seizure of papers for a criminal case.[261] At the same time, they are careful to note that some courts might have allowed seizure of very particular, contraband papers, such as seditious libels.[262] But in the view of Eric Schnapper and Donald Dripps, at least, government agents could not justify a rummaging through other papers in search of the seizeable one.[263]

Scholars such as Schnapper, Dripps, and Laura Donohue point to the unequivocal rejection of a wholesale seizure of papers in the *Entick* case as evidence of the thinking at that time. It was one case, but scholars agree that the *Entick* and *Wilkes* cases so dominated the colonial discussion concerning the seizure of papers—and searches and arrest more generally under general warrants—that they enjoy outsized influence.[264]

These scholars have also canvased numerous other contemporary sources to support the view that the Fourth Amendment bans the seizure and search of papers for a criminal case. Dripps points to the numerous pamphlets in England and also culls case law, statutes, and pamphlets from the colonies to support the view.[265]

On the other hand, Thomas Y. Davies contests the view that the framers intended the Fourth Amendment to ban paper searches, in part because they were unfamiliar with the version of the *Entick* case that included the

260. *See* Veeder v. United States, 252 F. 414, 418 (7th Cir. 1918) ("By exclusion, therefore, papers and documents which afford evidence that a felony has been committed, but which were not the means of committing it, are immune from seizure." (construing the predecessor to Rule 41)).

261. Donohue, *The Fourth Amendment in a Digital World*, *supra* note 6, at 560; Dripps, *supra* note 6, at 82–83; Schnapper, *supra* note 6, at 869–70.

262. *E.g.*, *Schnapper*, *supra* note 6, at 900–04.

263. *Id.* at 923; Dripps, *supra* note 6, at 101–02.

264. Donohue, *The Original Fourth Amendment*, *supra* note 6, at 1258–59; *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 767, 776 (1994); Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 980 (2016).

265. Dripps, *supra* note 6, at 68. For example, he places substantial reliance on one of Congress' first laws, Section 15 of the Judiciary Act of 1791, which, he says, implies law enforcement cannot compel the production of or seizure of papers for a criminal case. *See id.* at 81–83. Basically, this Act allows federal courts to compel discovery of a party's papers for the other side only to the extent allowed by the courts of equity, and these courts at the time did not allow papers to be compelled for criminal cases. In addition, the Act makes as punishment for a failure to produce papers a default judgment or nonsuit against that party—purely civil penalties that would not be relevant if the provision applied to criminal cases. Federal Judiciary Act, ch. 20, § 15, 1 Stat. 73 (1789). Richard Nagareda has pointed to the penalty portion as evidence that the Act excludes from its ambit criminal cases. Richard A. Nagareda, *Compulsion "to be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. Rev. 1575, 1622 (1999).

statements disfavoring paper searches.[266] This longer version of *Entick*, originally in Francis Hargrave's collection of cases,[267] was published in the United States only later, Davies argues.[268] But another commentator has shown that the longer version of *Entick* from Hargrave's collected cases did in fact appear in American libraries before the framing of the Fourth Amendment.[269] In addition, other sources do seem to envision paper searches with a warrant, such as the Virginia Ratifying Convention of 1788's recommendation for a bill of rights.[270]

Either way, this Article does not embrace a version of originalism that would have us adopt a particular and highly specific understanding of the open textured phrase, "unreasonable searches and seizures." First, a total ban on paper searches for criminal cases, even with a warrant, would exact too high a cost on ordinary investigations. In today's mature, sophisticated regulatory state, the ban, not the searches, would be unreasonable.

Second, even from the framers' perspective, we might not have a clear idea how they viewed the search for papers in ordinary criminal cases. After all, the *Wilkes* and *Entick* cases were political, not ordinary theft or murder cases, and the framers may have cabined those cases off in their minds from the run of the mill criminal case. Moreover, state statutes leading up to 1789 authorized warrants for cases of stolen goods or excise, imposts, or duties, but one reads little of warrants to seize papers in ordinary criminal cases.[271] This is not surprising since papers played a small to non-existent role as evidence in an ordinary criminal case. As David Sklansky has cautioned, we must guard against making concrete conclusions about the original meaning of the Fourth Amendment from simply a few cases, or practice—especially since the colonies each had their own common-law principles and practices.[272]

---

266. Davies, *supra* note 6, at 726–27; *see also* WILLIAM RAWLE, A VIEW OF THE CONSTITUTION OF THE UNITED STATES 127 (2d ed. 1829) (explaining that upon a proper warrant, "not only may other effects, but the papers of the accused be taken into the custody of the law"). Of course, this statement does not entirely answer whether the government may search all papers, even innocent ones, to find the one incriminating paper.

267. 11 FRANCIS HARGRAVE, A COMPLETE COLLECTION OF STATE-TRIALS AND PROCEEDINGS FOR HIGH TREASON AND OTHER CRIMES AND MISDEMEANOURS 313 (4th ed. 1781).

268. Davies, *supra* note 6, at 565 n.25.

269. Roger Roots, *The Framers' Fourth Amendment Exclusionary Rule: The Mounting Evidence*, 15 NEV. L.J. 42, 54–55 (2014).

270. NEIL H. COGAN, THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, & ORIGINS 233 (stating in Article XIV that a warrant to seize papers *not based upon oath or affirmation* would be oppressive and ought not to be granted); *see also* ST. GEORGE TUCKER, VIEW OF THE CONSTITUTION OF THE UNITED STATES WITH SELECTED WRITINGS 294 (Clyde N. Wilson ed., 1976) (rephrasing the Fourth Amendment, perhaps inadvertently, so as to envision searches of papers upon a proper warrant).

271. *See generally* CUDDIHY, *supra* note 210 (providing an analysis of the progression of the Fourth Amendment through 1791).

272. *See generally* David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739 (2000) (arguing that the Supreme Court's focus on an originalist interpretation of the Fourth Amendment does not actually follow from the text or the intent of the Fourth Amendment).

Third, even the scholars cited above do not argue that we should interpret today's Fourth Amendment precisely as the framers would have. They too look to the founding generation for guidance, not binding interpretation.[273] Nevertheless, we may advert to the apparent founding era ban on paper searches for important rhetorical purposes. For example, law enforcement often argues that any limit on searches of papers represents a new limit that must be justified. Instead, history makes clear that it is law enforcement that seeks greatly expanded search and seizure powers.[274]

C. INSTEAD OF A BAN—AN INVENTORY

Although we have stopped short of banning all paper searches for criminal cases, even with a warrant, we may still look to *Entick* for important clues to how the founding era *would have* governed paper searches. The court in *Entick* took an interesting rhetorical approach that helps us with this task. It wrote that paper searches must be illegal because, if they were legal, they would have several safeguards.[275] The lack of safeguards shows the common law did not envision such searches: "[A]ll these precautions would have been long since established by law, if the power itself had been legal."[276]

Even as it rejected paper searches, the court in *Entick* suggested what would be the proper checks were we to allow paper searches.[277] They included the requirements of "an exact inventory" and to deliver a copy.[278] Elsewhere, the court emphasizes the importance of the return—the return of the papers to the court that issued the warrant. As it was, the court complained, the warrant afforded the messengers the discretion to execute the warrant when Entick was not present to oversee the seizure and determine what they took. They could, for all the court knew, take bank bills (money), and Entick would have no recourse. The officers did not make a return of the warrant to a court with such an inventory. They did not make provision for Entick to recover his property.[279] In *Wilkes v. Wood*, the court similarly pointed to the lack of an inventory as problematic.[280]

The founding era thus supplies a few key lessons for today. First, the Fourth Amendment likely includes a requirement that officers create an inventory or return of the things they seize pursuant to a warrant. At the very least, the practice, cases, and statutes widely required such an inventory or

---

273. *See generally* Schnapper, *supra* note 6 (arguing "that the Supreme Court's original view of the history and meaning of the Fourth Amendment was correct").

274. Donohue, *The Fourth Amendment in A Digital World*, *supra* note 6, at 568.

275. *See* Entick v. Carrington, 19 Howell's St. Tr. 1029, 1067 (CP 1765).

276. *Id.*

277. *Id.*

278. *Id.* It is not clear who must create this inventory, a government official or a representative of the owner. The court uses the term "servant." *Id.*

279. *Id.* at 1066.

280. Wilkes v. Wood (1763) 98 Eng. Rep. 489, 498–99 (KB); *see also* Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders*, 93 WASH. L. REV. 145, 173–74 (2018).

return. Second, we cannot apply this inventory requirement directly to the seizure of papers because, unlike other things, the founding generation likely banned any seizure of papers in criminal cases, warrant or no warrant. Third, however, those same sources almost directly say that were we not to ban paper searches, at the very least we would need to inventory the papers seized for the search to be lawful. For the very same reasons that faced the founding generation, we can apply the same inventory requirement to files opened during a search of a device.

D. CONTRARY CASE LAW

On the other hand, cases primarily from the 1960s and 1970s challenge my view that the Constitution requires a return, inventory, or opportunity to get one's property back—though often in terse, single-sentence holdings. For example, the Supreme Court in *Cady v. Dombrowski* wrote in a single sentence that an incomplete inventory does not violate the Fourth Amendment.[281] Other cases have held that the Fourth Amendment does not require an inventory or return at all,[282] or even that the police give the individual back property it unlawfully seized.[283] These cases rely upon the proposition that once the police validly search for and seize property, the Fourth Amendment search and seizure provision no longer applies. An officer's failure to complete an inventory, coming *after* the search and initial seizure, therefore cannot violate the Fourth Amendment.[284] I show here why these cases were wrongly decided at the time and have been undermined by the Court's 2017 case *Manuel v. City of Joliet*.[285]

First, these cases were wrongly decided at the time, that is, in the 1960s and 70s. None of them addressed the history of the Fourth Amendment sketched above or the central role the return and inventory played in case law, statutes, and practice. Put another way, these courts assessed these warrant procedures entirely under the Reasonableness Clause. They reasoned that by the time of the return and inventory, the search and seizure have ended and the Fourth Amendment therefore no longer applies. But even were we to agree that the search and seizure have ended, and so has the force of the Reasonableness Clause, the Warrant Clause continues to exercise independent force.

After all, my proposal falls chiefly under the Warrant Clause and what constitutes a "warrant," as originally understood. The return, the inventory, and the right of an individual to have restored to him goods seized that were not described in the warrant all count as part of the warrant process in a continuous practice from the founding era to today.

---

281. Cady v. Dombrowski, 413 U.S. 433, 449 (1973) ("As these items were constitutionally seized, we do not deem it constitutionally significant that they were not listed in the return of the warrant.").

282. United States v. Dudek, 530 F.2d 684, 691 (6th Cir. 1976).

283. Denault v. Ahern, 857 F.3d 76, 83–84 (1st Cir. 2017) (collecting cases).

284. *E.g.*, *Dombrowski*, 413 U.S. at 449.

285. Manuel v. City of Joliet, 137 S. Ct. 911 (2017).

As already noted, the inventory and return formed so central a part of the warrant process as to constitute what the founders understood by the term "warrant." As Otis and Adams argued, the writs of assistance were bad precisely because they contained no return requirement.[286] As a matter of constitutional interpretation, the Court has not hesitated to find other common-law practices such as knock and announce[287] or a neutral magistrate[288] to be essential to the meaning of a warrant—based on founding era practice continued to this day—even though the text likewise does not expressly require them.

But the chief flaw in *Dombrowski*, *Dudek* and similar cases lies in their premise—once the officer has seized the items, the Fourth Amendment no longer governs.[289] It is this argument that confuses seizures with searches and that has been undermined most recently in 2017 by the Supreme Court's decision in *Manuel v. City of Joliet*.[290] It is true, of course, that once officers have left the home with seized items in hand, the *search* has already occurred, as have any harms occurring directly from the search such as invasion of privacy or trespass.

But even after completion of the search, the seizure continues beyond the initial taking of the items. In *Manuel*, the Court held that a person unlawfully arrested may still assert a Fourth Amendment right over her *continued* detention, not simply the initial seizure, even for weeks duration.[291] The Court noted that a "seizure" means a person is not free to leave, and when the police continue to detain a person, she is not free to leave.[292]

Similarly, the Fourth Amendment should continue to apply to the seizure of property after the initial taking. The Court has defined a seizure of property as a "meaningful interference with an individual's possessory interests in that property."[293] Retaining property interferes with possessory interests in that property in the same way as the detention of a person continues the seizure of a person. There is no escaping the analogy.

---

286. *See* Clancy, *supra* note 197, at 1058 (explaining that "writs of assistance were seen as deficient because, inter alia . . . they were not returnable").

287. Wilson v. Arkansas, 514 U.S. 927, 929 (1995).

288. Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 326 (1979).

289. *Dombrowski*, 413 U.S. at 449; Denault v. Ahern, 857 F.3d 76, 84 (1st Cir. 2017) (finding that the Fourth Amendment does not apply to retained property because the initial seizure was lawful); United States v. Dudek, 530 F.2d 684, 690 (6th Cir. 1976).

290. *Manuel*, 137 S. Ct. at 918.

291. *Id.* at 918–19; *see also* Gerstein v. Pugh, 420 U.S. 103, 114 (1975) (holding that a magistrate must determine there is probable cause before there is an "extended restraint of liberty following arrest"); Fontana v. Haskin, 262 F.3d 871, 879–80 (9th Cir. 2001) (individual could recover under the Fourth Amendment for officer's use of excessive force not only in the initial arrest but any time during the "continuing seizure" while in the arresting officer's custody).

292. *Manuel*, 137 S. Ct. at 917 ("'A person is seized' whenever officials 'restrain[ ] his freedom of movement' such that he is 'not free to leave.'" (alteration in original) (quoting Brendlin v. California, 551 U.S. 249, 254 (2007))).

293. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

Even Justice Alito's dissent supports my point that a Fourth Amendment seizure continues beyond the initial capture and up to a day or two. He conceded the seizure continues until an initial appearance before a judge —just not after. Indeed, this initial appearance before a judge under *Gerstein v. Pugh*,[294] or the presentment requirement under *McNabb v. United States*,[295] bear striking resemblance to the return and inventory requirement for property, both today and at the founding. In the founding era, a search warrant for stolen goods required the officer to bring the property *and* the suspect immediately to the justice of the peace to address both.[296] In each case, the requirement furthers accountability before a neutral judge rather than simply before an officer or at the behest of an interested complainant.

Third, these courts argue that the inventory and return requirements are merely "ministerial" or "technicalities"—apparently not at the core of the Fourth Amendment. This argument is particularly misplaced because a primary purpose of the Warrant Clause is to put the officer executing the warrant in a ministerial position even in conducting the search and seizure.[297] The premise is that the magistrate lists in the warrant the places to be searched and the things to be seized with sufficient particularity that the officer has no discretion. Rather, the officer simply follows the directions. As the Court stated in *Marron v. United States*: "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[298] This principle applies with particular force to the seizure of books and papers.[299]

Despite the ministerial nature of the search itself, courts treat the search as a substantive subject for inquiry and violation. The return and inventory can similarly be labeled ministerial, but that's no argument as to whether the requirement is *important*. Like the scope of the search, the return and inventory perform critical functions of supervision and accountability, whether or not we call them ministerial.

Fourth, these cases purport to be deciding whether the Fourth Amendment applies, but they are really concerned that the exclusionary rule not apply to the failure to create an inventory. They appear to believe that the only way to ensure the exclusionary rule does not apply is to hold that the Fourth Amendment itself does not apply. Throughout *Dudek*, for example, the Court spends more time explaining why it will not extend the exclusionary rule to this situation than it does analyzing whether the Fourth Amendment

---

294. *Gerstein*, 420 U.S. at 108–09.

295. McNabb v. United States, 318 U.S. 332, 342 (1943).

296. *E.g.*, JAMES PARKER, A NEW CONDUCTOR GENERALIS: BEING A SUMMARY OF THE LAW RELATIVE TO THE DUTY AND OFFICE OF JUSTICES OF THE PEACE, SHERIFFS, CORONERS, CONSTABLES, JURYMEN, OVERSEERS OF THE POOR, &C. &C 406 (Albany 1803) (providing that a search warrant by a justice of the peace should say, "you are to bring the goods so found, and also the body of the said O.O. before me").

297. *E.g.*, Marron v. United States, 275 U.S. 192, 196 (1927).

298. *Id.*; Horton v. California, 496 U.S. 128, 144 (1990) (quoting *Marron*, 275 U.S. at 196); Andresen v. Maryland, 427 U.S. 463, 480 (1976) (quoting *Marron*, 275 U.S. at 196).

299. Stanford v. Texas, 379 U.S. 476, 485 (1965); *see also* Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325 (1979).

should apply.[300] But we need not be driven by concerns over the exclusionary rule. Since those cases were decided, the Court has significantly unhinged the exclusionary rule from the Fourth Amendment. Now, unlike then, the exclusionary rule would likely not apply to an inventory requirement even if the Fourth Amendment does. For example, under *Hudson v. Michigan*, courts should not suppress evidence for a failed inventory because the failure of the inventory did not cause or allow the officers to obtain the evidence.[301] As a result, under today's standards, these older cases such as *Dudek* could have held that the exclusionary rule does not apply without needing to decide or hold that the Fourth Amendment does not.

VII. CONCLUSION

Courts regularly repeat their commitment to the privacy of papers, especially when they consider the "vast troves" of personal information on an electronic device. It has become a cliché. It has also become a cliché that these same courts proceed to impose nearly no limits on law enforcement searches of these devices once agents have obtained a warrant. Today's warrants have become general warrants, and yet, courts claim they are powerless, as a practical matter, to impose limits.

This Article demonstrates how courts can impose limits on warrants, both before the search via express terms in the warrant and, more importantly, after issuing the warrant by insisting upon a meaningful inventory of the files or other chunks of information viewed or copied. This Fourth Amendment inventory for digital evidence will impose a disciplining effect on agents, aware that the scope of their search will, for the first time, be transparent to courts and suspects. Any searches that exceed a reasonable scope could lead to suppression, or a civil lawsuit, for a Fourth Amendment violation.

The inventory will also further key Fourth Amendment values that go beyond the Court's sometimes simplistic concept of privacy-as-secrecy. It will further the security of information at the center of the provision by affording suspects transparency of what has been viewed and copied and power over what the government keeps, which is especially important to limit future searches for new crimes or other data mining.

These proposals are entirely new, and yet they have their roots directly in the originalist sources for the Fourth Amendment. They arise out of the founding generation's reverence for the privacy of papers. The crux of the inventory requirement draws upon those same originalist sources to show how an inventory requirement for ordinary property can afford substantial protections when applied sensibly to papers and electronic information.

300. United States v. Dudek, 530 F.2d 684 *passim* (6th Cir. 1976).

301. Hudson v. Michigan, 547 U.S. 586, 594–95 (2006).