MAKING WARRANTS GREAT AGAIN: AVOIDING GENERAL SEARCHES IN THE EXECUTION OF WARRANTS FOR ELECTRONIC DATA

December 2021

Contact person:

Jennifer Stisa Granick
Surveillance and Cybersecurity Counsel
American Civil Liberties Union
jgranick@aclu.org

MAKING WARRANTS GREAT AGAIN: AVOIDING GENERAL SEARCHES IN THE EXECUTION OF WARRANTS FOR ELECTRONIC DATA

Jennifer S. Granick

TABLE OF CONTENTS

MAKING WARRANTS GREAT AGAIN: AVOIDING GENERAL SEARCHES IN THE EXECUTION OF WARRANTS FOR ELECTRONIC DATA

Jennifer S. Granick[*]

October 2021

I. INTRODUCTION

In a trio of recent cases, the U.S. Supreme Court has acknowledged that the digital age requires reevaluation of Fourth Amendment doctrine to ensure that privacy survives that onslaught of new surveillance technologies. These cases generally require law enforcement officers to "get a warrant" before they search a cell phone, track someone's physical location, or obtain vast, sensitive, and revealing records about us from service providers. *See Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400, 416 (2012); *Carpenter v. United States*, 138 S. Ct. 2206 (2018). These recent precedents are vital. But the question of whether a warrant is required is not the only critical one. The next question, of equal importance, is "what does a warrant require?" For the Supreme Court precedent to adequately protect privacy, warrant protections must be robust.

The goal of this paper is to present legal arguments in support of requirements that would ensure that warrants meaningfully curtail the all-permeating surveillance enabled by new technologies.[1] Detailed exposition of these legal arguments is also contained in the multiple ACLU amicus briefs attached as an appendix.

This paper argues that some recommended practices are well-founded in existing Fourth Amendment law and that courts and investigators *must* follow them. *See, e.g.*, *infra* Section 4.A. The paper also recommends practices which *should* be constitutionally required given the special nature of electronic information and the role of the Fourth Amendment. Finally, there are some recommendations that are not necessarily required in every case, may nevertheless be *advisable* steps to ensure the government does not overstep constitutional

---

[*] Jennifer Stisa Granick is Surveillance and Cybersecurity Counsel with the ACLU's Speech, Privacy, & Technology Project, where she litigates and writes about privacy, security, technology, and constitutional rights, and leads the ACLU's advocacy on warrant protections under the Fourth Amendment. ACLU attorneys, fellows, interns, and paralegals provided invaluable contributions to this paper—Ashley Gorski, Brett Max Kaufman, Adeline Lee, Rachel Maremont, Nicola Morrow, Noam Shemtov, Patrick Toomey, Fikayo Walter-Johnson, Daniela del Rosario Wertheimer, Nate Wessler, and Ben Wizner.

[1] This memo is concerned with the permissible scope of warrants themselves, and does not address the antecedent question of which categories of information, such as location data or medical records, should require a warrant in the first place. It explains the ACLU's amicus advocacy on digital age warrants in state and federal courts, examples of which are attached as an appendix.

boundaries; imposition of limitations up front can help avoid subsequent Fourth Amendment violations.[2] *See, e.g.*, *infra* Section IV.B.5.

There are a number of ways in which current search warrant practice can improve:

- Probable cause to justify a search or seizure of electronic information must be based on facts specific to the investigation. But some courts have found probable cause on the mere basis that people, including criminals, frequently use their phones.
- Warrants should not authorize seizures of *all content* in an online account, and must only authorize seizures of entire digital devices for the limited purpose of promptly, and in conformity with demonstrated probable cause, locating responsive evidence.
- Law enforcement must execute searches in a manner designed to guard against exposure of private information intermingled with potentially relevant evidence. (Data seized without probable cause as a matter of administrative convenience is called "non-responsive data".) Yet, some courts have been extremely permissive once police seize data, largely accepting government claims that investigators need substantial leeway because electronic information is easily destroyed, hidden, or otherwise manipulatable. These courts have permitted investigators to rummage through voluminous information often without direction or limitation. This happenstance method of querying data is both unconstitutionally invasive and counterproductive in practice.
- Courts must ensure that data is deleted when it is no longer relevant to the case or when the case is terminated. Lawfully held but non-responsive data must not be searched or otherwise used, at least not without getting a second warrant, and then only when the ongoing retention of the data is reasonable. People retain an expectation of privacy in their data seized by law enforcement, especially the non-responsive data for which there is no probable cause to search. Yet, storage is cheap and some police departments are unlawfully retaining seized information indefinitely and using it in subsequent investigations, essentially keeping a permanent dossier that can include information about suspects, victims, witnesses, and other innocent third parties.

[2] These recommendations raise the question of the scope of magistrate authority in regulating searches and seizures. Some scholars have argued that magistrates do not have broad authority to impose pre-search limitations on officers, while others have disagreed. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1278–84 (2010); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1 (2011). Without question, magistrates have the power and the obligation to deny warrants to search or seize data for which there is no probable cause.

II. SEARCHES OF ELECTRONIC DATA ARE IN DANGER OF BECOMING THE MODERN-DAY EQUIVALENT OF GENERAL WARRANTS

A. PRIVATE DIGITAL DATA IS VOLUMINOUS AND EXTREMELY SENSITIVE

Today, a massive amount of revealing, personal information is stored on our computers and cell phones, and "in the cloud," on Internet-connected servers hosted by the scores of online companies whose products and services we use on a daily basis. Modern computers, including cell phones, "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. . . . [M]any of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 573 U.S. at 393. Digital information generated by today's devices and services reveals individuals' private matters far beyond what one could learn from physical analogs. *Id.* at 394. A device the size of a human palm can store practically unlimited quantities of data. *Id.* For example, sixteen gigabytes of information—the standard capacity of a smart phone around the time the Court decided *Riley*—"translates to millions of pages of text, thousands of pictures, or hundreds of videos." *Id.*

Our cell phones track what we read and buy, where we go, and increasingly, they can reveal what we think. Today, people who carry cell phones, use social media, or take advantage of online storage generate a vast quantity of sensitive and private information. A search of even one device is deeply invasive. *See United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information.").

Online accounts are even more extensive. Google offers fifteen gigabytes of data storage for free, and up to two terabytes (2,000 gigabytes) of storage at negligible cost. *See* Google, *About Google One*, https://one.google.com/about. Google's servers store volumes of data, including email, photos, videos, calendar items, documents and spreadsheets, videos watched, search terms entered, websites visited, and the locations users have been to while carrying their phones. These accounts contain people's most intimate and private documents—love notes, tax records, business plans, health data, religious and political affiliations, personal finances, and digital diaries, to name just a few.

Police access to social media accounts and online communications services present a "threat [that] is further elevated . . . because, perhaps more than any other location—including a residence, a computer hard drive, or a car—[social media accounts] provide[] a single window through which almost every detail of a person's life is visible." *United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (describing Facebook).

Treating digital searches the same as analog ones is "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 573 U.S. at 393.

B. ELECTRONIC STORAGE INTERMINGLES DATA THAT THERE IS PROBABLE CAUSE TO SEARCH WITH SENSITIVE, NON-RESPONSIVE INFORMATION

In the age before computers, searches generally involved physical spaces, which have intuitive natural limits. Officers may look in only those places large enough to hold the physical items particularly described in the warrant. So, police cannot open a spice box when searching for a rifle. *See, e.g.*, *Horton v. California*, 496 U.S. 128, 141 (1990). Nor can they rummage through a medicine cabinet to look for a flat-screen television. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013).

These physical limitations are nonexistent in the digital context. Computer hard drives and online services intermingle huge amounts of personal information, both irrelevant material and, potentially, evidence of criminal behavior. Some data sets involve personal data of people other than the suspect, who are uninvolved in any wrong-doing. Social media accounts involve conversations with and between friends. Internet data flows can include email messages from multiple people's inboxes. Depending on where the collection happens, the number of people affected by a single warrant could be in the hundreds (social media) or the millions (Internet backbone taps). How can police meaningfully and efficiently search all this data for evidence of a crime without revealing all of the target's data and too much information about uninvolved third-parties? How should the law protect people from opportunistic invasions into their private affairs merely because they communicated with or near a suspect?

This is not an entirely new challenge, as filing cabinets may also intermingle responsive and non-responsive documents. *See Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). But the problem is exacerbated by the volume and scope of digital storage. As storage gets cheaper and more devices gather data about us, the challenge gets harder.

Understanding the forensic search process leads to the following conclusion: In most instances the government will overseize data, especially when stored on hardware devices such as phones and laptops. It is all the more important, then, for courts to insist that investigators conduct narrow and refined searches, and carefully document their queries and the scope of their searches. Moreover, there must be limitations on how the government may access, store, and use non-responsive data, lest device searches become general warrants in practice.

III. THE DIGITAL FORENSIC PROCESS GENERALLY INVOLVES OVERSEIZURE OF DATA FOLLOWED BY TECH-ASSISTED QUERIES

Forensic analysis of electronic devices presents challenges to compliance with traditional Fourth Amendment doctrine. To understand these challenges, readers need a basic working knowledge of digital forensics. As law enforcement conducts investigations involving digital data they go through a series of separate actions that each may constitute searches or seizures and thus implicate the Fourth Amendment. At a high level, these include hardware seizure, data copying, data querying, and data storage, distribution, and retention.

A. HARDWARE SEIZURE

When executing a warrant for electronic evidence, investigators will typically start by seizing the hardware—a computer, cell phone, or other storage device like a USB drive or

an SD card. Hardware seizures generally require a warrant, and most often the basis for probable cause is that evidence will be found on the device. Only rarely are hardware seizures based on the claim the device itself is evidence or an instrumentality of the crime.

Warrants must be particularized and not overbroad, but seizing an electronic device will inevitably put far more data in government hands than is relevant to probable cause. Nevertheless, investigators rarely search the devices on site. They may create a digital copy to search later. But more commonly, they take all physical devices for later data analysis.

Investigators usually justify these hardware seizures on the grounds that searching stored data onsite is too time consuming and, without proper forensic tools and procedures, can interfere with the integrity of any evidence that investigators might find.[3] Because forensic analysis takes time and special equipment, conducting a thorough and forensically sound investigative search will usually take too long to conduct on the premises. *See, e.g.*, *United States v. Hill*, 459 F.3d 966, 974–75 (9th Cir. 2006) ("[T]he process of searching the files at the scene can take a long time. . . . Police would have to be present on the suspect's premises while the search was in progress."); *Guest v. Leis*, 255 F.3d 325, 334–35 (6th Cir. 2001) (citing cases from the First, Ninth, and Tenth Circuits) ("In the instant cases, when the seizures occurred, defendants were unable to separate relevant files from unrelated files, so they took the computers to be able to sort out the documents off-site. Because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files."); *see also* Comput. Crime and Intell. Prop. Section, Crim. Div., U.S. Dep't of Just., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 77–78 (3d ed. 2009), available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf ("Because examining a computer for evidence of crime is so time consuming, it will be infeasible in almost every case to do an on-site search of a computer or other storage media for evidence of crime. . . . In many cases, rather than seize an entire computer for off-site review, agents can instead create a digital copy of the hard drive that is identical to the original in every relevant respect.").

Many courts have accepted device seizure as reasonable under the Fourth Amendment, even though it routinely means overseizing the data stored on the device. *See, e.g.*, *United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) ("[W]here there was ample evidence

---

[3] For example, if a computer disk is mounted as "read/write," then the computer will make many normal changes to it, updating timestamps and local indexes, and more. Hardware tools called "write blockers" or "forensic disk controllers" let an investigator make a copy of a source disk (or equivalent) without changing the seized disk. *See generally Forensic Disk Controller*, Wikipedia, https://en.wikipedia.org/wiki/Forensic_disk_controller. There are also software equivalents that in the software driver allow reads but not writes. Sometimes, a law enforcement officer will scroll through data on a cell phone at the scene without first making a forensic copy. This is not a best practice because it alters data on the device. With both computers and mobile devices, searches should take place only on the forensic copy. Moreover, investigators should securely store an exact or "mirror" copy in case there are any questions about the authenticity of the data.

that the documents authorized in the warrant could be found on a person's computer, the officers did not exceed the scope of the warrant when they seized the computer."). These courts have opined that the "reality [is] that over-seizing is an inherent part of the electronic search process." This is because the government may need to seize the hardware first in order to conduct an exhaustive search of the data stored on it later. *See, e.g.*, *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012).

While seizing hardware makes sense in many cases, the Fourth Amendment does not give the government a "blank check" when seeking or executing warrants in computer-related searches. As the Ninth Circuit has stated, "[a]lthough computer technology may in theory justify blanket seizures . . . the government must still demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand." *Hill*, 459 F.3d at 975. Increasingly, it may not be. For example, in the recent case of *Commonwealth v. Green*, the crime was committed using uTorrent software. Police obtained a very broad warrant authorizing seizure of all computer hardware. With a mobile forensic tool, however, the police were able to quickly examine the hardware and identify a subset with uTorrent stored on it. The police then took those devices, leaving the remainder behind. 204 A.3d 469, 482 (Pa. Super. Ct. 2019), *appeal granted in part* 243 A.3d 1293 (Pa. Jan. 25, 2021).

B. DATA SEIZURE

Once law enforcement seizes a physical device, the first step in a forensic search is to obtain an exact or "mirror" copy of the data.[4] Often this entails sending the physical media to a forensic crime lab for use of special software that properly copies the data.

---

[4] Nat'l Insts. of Just., Forensic Examination of Digital Evidence: A Guide for Law Enforcement 1 ("Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a ***copy*** of the ***original evidence***. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence."); Gary Kessler & Gregory Carlton, *A Study of Forensic Imaging in the Absence of Write-Blockers* 51, J. Digit. Forensics, Sec. & L. (2014), https://doi.org/10.15394/jdfsl.2014.1187 ("What happens if a disk or other media is imaged without benefit of a write-blocker? Is the copy tainted? If so, what is the extent of any contamination? Procedurally, if a device is imaged without a write-blocker, should such evidence be discarded by an examiner or investigator, ignored by counsel, or challenged by the opposing party on the presumption that the image no longer represents the original media? If such a generalized objection were raised, how should a judge know whether to sustain or overrule the objection, and how should the party offering such evidence argue for the evidence's inclusion? These questions are not entirely hypothetical."); The Official CHFI Study Guide 618 (Dave Kleiman et al. eds., 2007), *available at* https://bit.ly/3Euw0ok ("The purpose of creating an evidence file is to have a copy of a suspect's media so the investigator does not contaminate the original media. If the original media were investigated instead of the evidence file, a savvy attorney could argue that the investigator altered the media to incriminate their client. Creating the evidence file helps to ensure that the examined media has not been tainted by an investigator.").

Surprisingly, it is not settled law that this data copying is a seizure.[5] It should be. Copying, even without reviewing, interferes with the owner's possessory interest in the information, including the ability to delete.

Information may also be seized from an online service provider such as Facebook or Twitter (social media posts and direct messages), Dropbox, Google Drive, Microsoft's OneDrive, and Apple's iCloud (cloud-stored files and hardware back-ups), or ATT, Comcast, Google search and Gmail, and more (location data, email, contact lists, IP address logs, search histories, browsing histories, etc.). In this cloud-data context, police send a copy of the search warrant or other court order to the electronic communications platform, and the platform conducts a search for relevant information. The service provider then discloses the responsive information to law enforcement.[6] Given the amount of private information stored in an online account, the disclosure can be voluminous, highly sensitive, and mostly irrelevant to the investigation. Nevertheless, officers are typically reluctant to have the provider discriminate between responsive and non-responsive information. There are means to mitigate overseizure in this context, but courts have so far imposed those measures only rarely. They must do so, as discussed in more depth below.

C. DATA EXTRACTION

The next step in obtaining information from hardware devices is to extract information from the device. Modern forensic technologies use several means of extracting data. In "manual extraction," an investigator views a device's contents like a normal user.[7] For example, investigators may take photographs or screenshots of a phone screen, email data to themselves from the phone, or video record their exploration of a phone's contents, to prove that data was actually found on the phone. "'Logical extraction' automates what can be done through manual extraction. In other words, it automatically extracts data that's presented on the phone to the user."[8]

---

[5] Note, *Digital Duplications and the Fourth Amendment*, 129 Harv. L. Rev. 1046 (2016) (summarizing different academic viewpoints).

[6] Where there is trust between the service provider and law enforcement, police do not seize computer servers, a practice which would implicate the privacy rights of the services' other users. Where investigators do not trust the service provider, they may threaten to seize business assets, or otherwise interfere with the operations of the business, including by violating the privacy of other users. *See, e.g.*, Michael Phillips, *Lavabit and the Right to Private E-mail*, The New Yorker (Oct. 13, 2013), https://www.newyorker.com/tech/annals-of-technology/lavabit-and-the-right-to-private-e-mail (court ordered email service to turn over decryption keys in investigation of a single email account even though keys would enable the government secretly to read the e-mails of all customers).

[7] *See* Logan Koepke et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 2, Upturn (Oct. 21, 2020), *available at* https://www.upturn.org/reports/2020/mass-extraction/.

[8] *Id.*

"File system extraction" allows investigators to get information in internal databases and other data that a device doesn't typically display to users. "Physical extraction" copies data bit-by-bit as it's physically stored on the phone's hardware, instead of as distinct files. To be legible to investigators, the data from a physical extraction must be restructured as files. Mirror copies are physical extractions.

File system and physical extractions enable more robust searches than a user generally can conduct by way of a machine operating system. Investigators create a working copy in which forensic software may recover deleted files, index texts, and compute unique identifiers for applications or other files.[9] Note that in file system and physical extractions, the extracted version of the data may include deleted items, along with metadata describing that an item as deleted, as well as other information beyond what a user can typically see.[10] Information obtained from service providers is generally produced in a format that investigators can search and read without a second "extraction" step.

D. DATA SEARCH

After law enforcement seizes data pursuant to a warrant, the law permits agents to search it for evidence of the crime at a later date. Rather than routinely get two warrants, one to seize and a second authorizing a later search, Federal Rule of Criminal Procedure 41 appears to embrace a two-step procedure of "seize first, search second." Section (e)(2)(B) states:

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

Next, investigators examine the extracted data, which includes the voluminous amount of revealing information that is irrelevant to probable cause. In our experience, officers have not constrained their searches to limit exposure of information to only that relevant to probable cause. In some cases, officers have manually examined files, clicking on files and documents at their own discretion. In other situations, officers have searched the data for evidence of different or new crimes. Officers generally do not keep search logs, nor do police departments appear to delete irrelevant information. The result is that searches end up being very broad, undermining the Fourth Amendment's purpose of protecting private information while allowing investigations limited by probable cause and subject to judicial oversight.

Manually examining files makes little sense from either a constitutional or an investigative perspective. Manual searches are impractical because there is so much information to go

---

[9] Nat'l Insts. of Just., *supra* note 4, at 16.

[10] *See* Koepke, *supra* note 7, at 21& n.42, 22 & n.43–45 ("Mobile device forensic tools can sometimes access 'deleted' data . . . [, but] access to deleted data depends on a range of factors, including phone hardware, encryption design, and extraction method.").

through; making sense of even a relatively small data set, like an email inbox, benefits from automated search. Moreover, randomly opening files means a human investigator is likely to examine private information for which there is no probable cause, and that is in law enforcement possession only because of administrative convenience. Whatever search technique law enforcement uses, the goal must be to effectively winnow down the huge amounts of data on a disk to only the information most likely to be relevant to the investigation. Doing so not only serves law enforcement's interests in efficiency and economy of investigatory resources; it is also essential to ensure constitutional compliance.

Investigators frequently use forensic software designed for digital investigations. Forensic software preserves information like filename and file location, but also aggregates every file found into a searchable and filterable pool. Law enforcement can then sort all available data by the time and date of its creation, by location, by file or media type, or by source application. Forensic software also allows examiners to pull all pictures or videos from the phone to view in one place—for example, as a grid of thumbnails or icons—regardless of how they are actually organized or named on the device. Officers can identify an image file masquerading as text, or a text file that also contains an image. *See, e.g.*, *Hill*, 459 F.3d 966 ("Images can be hidden in all manner of files, even word processing documents and spreadsheets."). Forensic tools can also search for key terms across the entire device, just as one might use Google to search the web, and display information about the results and where on the device they're from. Investigators can refine their queries using keyword searches, including Boolean queries like those lawyers use in a Westlaw search.

Forensic software tools can perform "fuzzy searches," which return information based on a calculation of probability rather than an exact match.[11] For example, the Blacklight tool claims the ability to categorize both still images and videos into various pre-defined categories: Alcohol, Child Sexual Abuse Material (CSAM),[12] Currency,

[11] The relationship of "fuzzy" searches to probable cause is complicated. All probabilistic matching implicitly has false positives (things that match, but erroneously) and false negatives (things that do not match, but should). If an algorithm is set to report positives with twenty percent certainty, does a hit constitute probable cause to open that file?

[12] This refers to a machine learning–aided "fuzzy" search where the software generates a prediction about the content of an image, which will generate false positives and negatives, but has the benefit of being able to classify previously unknown illicit images. A more common means of searching for known CSAM images is to a create hash value for each image, a string of uniquely identifying letters and numbers. Investigators then use the same mathematical process to calculate hash values for unknown files on a device to be searched. If one of the files on the device has an identical hash to a known CSAM image, it is identical to that image. This is a means of quickly searching a voluminous number of files for a known image.

Documents,[13] Drugs, Extremism, Gambling, Gore, ID/Credit Cards, Porn, Swimwear/Underwear, and Weapons.[14]

Like any search technique, forensic search tools can be over- or under-inclusive. But because forensic tools can extract more and different types of data, and analyze it far more efficiently, they are significantly different from manually searching a cellphone or computer hard drive. They can reveal information that the owner does not know is there, and, by gathering hidden and deleted files, exacerbate the potential for indiscriminate and overbroad searches. As with manual searches, forensic searches potentially expose substantial amounts of irrelevant info to manual review by investigators. For this reason, some technical expert have concluded that forensic search tools "are simply too powerful in the hands of law enforcement and should not be used."[15]

The ACLU has argued that, properly regulated, forensic tools can be used in ways that *reduce* rummaging, limit law enforcement agents' exposure to non-responsive information, and enable judicial oversight and auditing of the search process.

E. POST-SEARCH

There is very little public information on what law enforcement agencies generally do with the digital information they seize, including once a case is over and especially in the absence of an affirmative request for the data to be returned or destroyed. We do not know how law enforcement segregates "raw data" from "responsive data," how data is stored, or whether and how it is disseminated. Nor do we know whether any of the seized information from a case is stored in a database where other investigators can potentially access it on an ongoing basis or for purposes that exceed the scope of the original investigation.

The little we do know is alarming. For example, it appears that the FBI has fed "raw" return data from an email search warrant into a centralized, searchable database called BIDMAS, including data obtained by other law enforcement agencies. Letter from AUSA to Hon. Allison J. Nathan at 2 (Oct. 30, 2020), *United States v. Nejad*, No. 1:18-cr-00224-AJN, 2020 WL 3057755 (S.D.N.Y. June 9, 2020), ECF No. 392 (hereafter "BIDMAS Letter"). The agency then searched this raw data hundreds of times in ways that were not authorized by the original search warrant, including in other investigations. *Id.* at 3.

In a number of cases, information obtained pursuant to one search warrant has been retained and used in subsequent investigations, including without a second warrant. *See, e.g.*, *United States v. Ganias* (*Ganias II*), 824 F.3d 199 (2d Cir. 2016) (en banc). This is problematic for several reasons. First, warrants may authorize searches only for evidence

---

[13] It is unclear what the category of "document" means in this context. The Blacklight manual lists the category without further explanation.

[14] Blackbag, *BlackBag Releases BlackLight 2019 R1 With Powerful New Features* (Apr. 24, 2019), https://www.blackbagtech.com/press-releases/blackbag-releases-blacklight-2019-r1-with-powerful-new-features/

[15] Koepke, *supra* note 7, at 5. The Upturn report recommends at a minimum banning consent searches of mobile devices, abolishing the plain view exception for digital searches, requiring easy-to-understand audit logs,

of the crime for which the government has established probable cause. So subsequent searches for evidence of separate crimes are unconstitutional, at least without a second warrant. Moreover, the Fourth Amendment applies to protect privacy and property interests in digital information that persist post-seizure. At some point in time, it becomes unreasonable (and therefore unconstitutional) to continue to retain seized data. *See infra* Section VI.B.8.

IV. THE FOURTH AMENDMENT'S PARTICULARITY AND PROBABLE CAUSE REQUIREMENTS DOCTRINALLY LIMIT DIGITAL SEARCHES AND SEIZURES

As digitization lowers the practical barriers to extreme privacy invasions and investigatory overreach, courts must ensure that constitutional protections against all-permeating government surveillance continue to apply to new technologies. The Fourth Amendment plays a critical role in this project. In applying its protections to novel technologies, the Supreme Court has recognized the importance of ensuring that the longstanding balance between the power and authority of the state and the privacy and liberty of the individual is not upset, either suddenly or through technological creep. *See, e.g.*, *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (The Fourth Amendment analysis asks whether the police conduct threatens to disrupt the traditional "relationship between citizen and government in a way that is inimical to democratic society") (internal quotation marks and citation omitted). To protect highly private and sensitive electronically stored information and avoid unnecessary exposure of our intimate details to investigators, warrants must strictly impose traditional Fourth Amendment limits on law enforcement's electronic searches and seizures.

The Fourth Amendment protects electronic information and devices. Its specification of "papers" and "effects" includes digital "papers" and electronic devices. *See Hoffa v. United States*, 385 U.S. 293, 301 (1966) (Fourth Amendment protections are "surely not limited to tangibles"). Individuals also have a protected privacy interest in the contents of their communications, including their telephone calls and emails. *See United States v. U.S. District Court* (*Keith*), 407 U.S. 297, 313 (1972); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).[16] Infringement of that privacy or interference with the property right constitutes a search or a seizure regulated by the Fourth Amendment.

---

[16] In a number of recent cases, the Department of Justice has argued that there is no reasonable expectation of privacy in email, and thus no Fourth Amendment protection, because provider policies state that the company will monitor for abuse of the service. *See, e.g.*, *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021); *United States v. Ackerman*, No. 13-10176-01-EFM, 2014 WL 2968164, at *8 (D. Kan. July 1, 2014), *reh'g denied*, 831 F.3d 1292, 1309 (10th Cir. 2016); *United States v. Basey*, No. 18-30121 (9th Cir. mandate issued Oct. 1, 2019) [attached at Appendix 685]; *United States v. Cobb*, 970 F.3d 319 (4th Cir. 2020) [attached at Appendix 354]. The Department of Justice subsequently abandoned this argument in *Wilson*, 13 F.4th 961 (9th Cir. 2021), however this issue is pending in other appellate courts. It contravenes long-standing prevailing wisdom. *See Carpenter*, 138 S. Ct. at 2222 (maj. op.) (in which every Justice agreed, at least in dicta, that the Fourth Amendment protects the content of emails); *id.* at 2230 (Kennedy, J., dissenting); *id.* at

Searches and seizures conducted without a warrant are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967) (footnotes omitted). Warrants are intended to prevent general searches, *Groh v. Ramirez*, 540 U.S. 551, 561 (2004), and to avoid a "general, exploratory rummaging in a person's belongings," *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

To obtain a warrant, law enforcement must demonstrate ***probable cause*** to believe that a crime was committed and that evidence of the crime will be found in the place to be searched or the thing to be seized. Probable cause to search exists when the totality of circumstances indicates a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

In addition to probable cause, neither warrants nor the searches they authorize may be ***overbroad***. A warrant is overbroad when it purports to authorize searches or seizures of places or things for which there is not probable cause to believe evidence will be found. Preventing overbroad searches by government agents was a central concern motivating the framers of the Fourth Amendment. In the American colonies, British agents used general warrants and "writs of assistance" to conduct broad searches for smuggled goods, limited only by the agents' own discretion. *See Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley v. California*, 573 U.S. 373, 403 (2014).

An affidavit supporting a search warrant must indicate "that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. There must "be a nexus . . . between the item to be seized and criminal behavior." *Warden, Md. Penitentiary v. Hayden*, 387 US 294, 307 (1967); *accord United States v. Brown*, 828 F3d 375, 382 (6th Cir. 2016) (requiring that affidavits must set forth "sufficient facts demonstrating why the police officer expects to find evidence in the [place to be searched] rather than in some other place") (citation omitted).

Related to overbreadth, warrants must ***particularly describe*** the things to be searched and seized. These two concepts are often confused. While the overbreadth rule places a substantive limit on the searches and seizures that a warrant may properly authorize—prohibiting magistrates from issuing warrants to search places or seize evidence for which law enforcement has not shown probable cause—particularity requires the warrant to state those limits clearly enough so as to cabin officer discretion in conducting the search or seizure. Warrants must serve as a practical guide for officers, allowing them to use rational judgment to distinguish between items that are responsive or not responsive to the warrant. The amount of specificity required is necessarily flexible: The type of crime, the facts already known by the officers, the facts that should be known by the officers, and other

---

2262, 2269 (Gorsuch, J., dissenting). *See also Warshak*, 631 F.3d at 283–84. It is disturbing that in 2021 the DOJ still will not commit to obtaining a warrant for communications content.

considerations all serve to set the bounds of what is sufficiently particular on a case-by-case basis. *See United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013); *United States v. Richards*, 659 F.3d 527, 537 (6th Cir. 2011) (quoting *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001)).

Courts must apply Fourth Amendment law stringently to address the unique attributes of digital data. "The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (collecting cases); Galpin, 720 U.S. at 446; see *also Berger v. New York*, 388 U.S. 41, 56 (1967) ("The need for particularity . . . is especially great" where the method of surveillance "involves an intrusion on privacy that is broad in scope."). The particularity requirement is especially important when the privacy interests in the place to be searched are highly sensitive. In *Stanford*, for example, the Supreme Court explained that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain." 379 U.S. at 511–12.

Despite these relatively straightforward principles, courts have struggled with how to apply Fourth Amendment law in the context of digital searches and seizures. Faced with the complexity of electronic searches, many courts have strayed from traditional Fourth Amendment doctrine. These struggles have produced opinions misguidedly blessing warrants for electronic information that are *less*, not more, rigorous than warrants of old, and searches of electronic data that are *more*, not less, expansive; all this despite the intimate, sensitive nature of electronic data. Today's warrants can come perilously close to the reviled general warrants that motivated the Fourth Amendment.

V. MAKING WARRANTS MEANINGFUL

A. DATA SEIZURES

This section makes the following claims:

- Courts must require a factual nexus between electronic devices/data and the investigation, and should not assume probable cause to search or seize electronic data exists in every case.
- When issuing warrants authorizing the seizure of electronic data stored online, courts must limit the seizure by particularly describing the category or types of data, the date range, and by imposing other filters on the data search.
- Warrants must limit the categories of data to be seized from social media or cloud-storage accounts to those responsive to probable cause.
- Warrants must require service providers to filter within categories, including date limitations, to further narrow the amount of non-responsive data law enforcement officers seize.

1. People Have a Property Interest in Electronic Data Such That Copying it and/or Retaining it Constitutes a Seizure.

The Fourth Amendment protects an individual's possessory interest in her papers and effects. *See Soldal v. Cook Cty.*, 506 U.S. 56, 62–64, 68 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched). Possessory interest is defined as the present "right to control property, *including the right to exclude others*, [even] by a person who is not necessarily the owner." Black's Law Dictionary (10th ed. 2014) (emphasis added); *United States v. 1982 Sanger 24' Spectra Boat*, 738 F.2d 1043, 1046 (9th Cir. 1984); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."). A possessory interest also includes the right to delete or destroy one's property. *United States v. General Motors Corp.*, 323 U.S. 373, 378 (1945) (property rights in a physical thing have been described as the rights "to possess, use and dispose of it" (quotation marks omitted)); *cf. United States v. Carpenter*, 484 U.S. 19, 26 (1987) ("Confidential business information has long been recognized as property.").

Electronic files possess these canonical characteristics of property. Users have the right to exclude others from their accounts. Users protect their accounts with passwords. Providers encrypt user emails both in transit and when stored on servers in order to exclude outsiders. Email users also have the right to delete their email messages; providers allow users to delete single messages, or the entire account. And even though email is intangible, it is still property subject to Fourth Amendment protections. *Hoffa*, 385 U.S. at 301 (Fourth Amendment protections are "surely not limited to tangibles"); U*nited States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir.1986) ("[S]urreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment."); *Katz*, 389 U.S. at 353; *Berger v. New York*, 388 U.S. 41, 54–60 (1967) (telephone conversations); *United States v. Biasucci*, 786 F.2d 504, 509–10 (2d Cir. 1986) (video surveillance); *United States v. Torres*, 751 F.2d 875, 883 (7th Cir. 1984) (video surveillance); *United States v. Taborda*, 635 F.2d 131, 139 (2d Cir. 1980) (enhanced visual surveillance inside the home). Moreover, the Fourth Amendment protects emails even if a provider's terms of service or privacy policy allow government access under certain circumstances, as almost all do.

Because email is private personal property, it is protected by the Fourth Amendment from unreasonable searches and seizures. Courts have considered and rejected arguments to the contrary. *See, e.g.*, *Warshak*, 631 F.3d at 286 ("While . . . a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . we doubt that will be the case in most situations . . . ."); *United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (policies establishing limited instances of access do not vitiate Fourth Amendment interests).[17]

A seizure occurs when police secure or detain private property so that they may search it later. The Fourth Amendment protects property from seizure even where there is a no

[17] For references to state law establishing that electronic data is property, *see* Brief of the ACLU and ACLU of Alaska Foundation, *United States v. Basey*, No. 18-30121 (9th Cir. filed Aug. 14, 2019) [attached at Appendix 646–85].

corresponding privacy or liberty invasion. *Soldal*, 506 U.S. at 62–65 (dragging away a mobile home was a seizure even though officers had not entered the house, rummaged through the possessions, or detained the owner). Similarly, in *United States v. Place*, 462 U.S. 696 (1983), officers seized a container and did not allow anyone to touch it or its contents while the police obtained a search warrant. This was a seizure governed by the Fourth Amendment. *Place*, 462 U.S. at 707 ("There is no doubt that the agents made a 'seizure' of Place's luggage for purposes of the Fourth Amendment when, following his refusal to consent to a search, the agent told Place that he was going to take the luggage to a federal judge to secure issuance of a warrant."). Likewise, private account data is seized at the moment that the government copies it, or demands that providers copy and preserve it.

2. Courts Must Require a Factual Nexus Between Electronic Devices/Data and the Investigation and Not Assume Probable Cause to Search or Seize Electronic Data Exists in Every Case.

The fact that evidence of a crime is often found in a particular location does not supply probable cause to believe that it will be found in that location in any particular case. For example, drug dealers often keep controlled substances in their homes, purses, or cars. But police are not generally permitted to search these places without investigation-specific reasons to believe evidence will be found there. The case *United States v. Brown*, 828 F.3d 375 (6th Cir. 2016), illustrates the proper application of the probable cause and particularity requirements of a warrant application. In *Brown*, the Sixth Circuit suppressed evidence obtained pursuant to a search because the affidavit in support of the warrant request "failed to establish the required nexus between the alleged drug trafficking and Brown's residence." *Id.* at 385. The connection "must be specific and concrete, not 'vague' or 'generalized.'" *Id.*

Therefore, probable cause to issue a warrant to seize electronic information must be based on case-specific facts and not general assertions: not every crime involves use of a cell phone, computer, social media account, or other online service. Our research shows that affidavits in support of search warrants often allege that, in the officer's experience, people who commit a particular crime use their phones to communicate about that crime or take pictures that could constitute evidence.[18] The affidavits commonly lack case-specific

[18] *See, e.g.*, *People v. Hughes*, 958 N.W.2d 98, 110 n.6 (2020) (Mich. 2020) [attached at Appendix 35] (court did not decide whether, in drug trafficking investigation, affidavit filed in support of warrant to search the defendant's cell phone provided only that in the officer's "training and expertise," drug dealers commonly use their phones in connection with their crimes provided sufficient nexus to establish probable cause); *Commonwealth v. Snow*, 160 N.E.3d 277 (Mass. 2021) [attached at Appendix 568] (sufficient evidence of a nexus between the crime and the device on those facts, but noting that neither evidence of a joint venture crime in which the participants all owned cell phones nor using a cell phone just prior to or during arrest would, in the absence of other evidence, provide probable cause); *United States v. Brown*, 828 F.3d 375, 384 (6th Cir. 2016) ("[I]f the affidavit fails to include facts that directly connect [a] residence with the suspected drug dealing activity, . . . it cannot be inferred that drugs will be found in the defendant's home—even if the defendant is a known drug dealer."); *cf. United States v. Hathorn*, 920 F.3d 982, 985 (5th

reasons to believe that evidence of the crime under investigation will be found on the particular devices or services. Despite this, magistrates often issue search warrants based on these thin, generalized assertions.

To meet their burden under the Fourth Amendment, investigators must attest to facts specific to the investigation that suggest electronic information will reveal evidence of the crime under investigation. While officers' training and experience can often be a basis for probable cause, there nevertheless needs to be some specific connection to the investigation underway, and not merely a general assertion that would apply to any and all such crimes.

Some examples: In *United States v. Lyles*, 910 F.3d 787, 794–95 (4th Cir. 2018), the warrant at issue authorized the search of a laundry list of electronic devices, including a cellphone, but failed to specify any particularized facts connecting the phone recovered in the search to the alleged criminal activity. *Id*. Instead, the affidavit for the warrant merely asserted that the home where the phone was recovered was connected to drug trafficking because "trash pulls" revealed evidence of marijuana possession and distribution. *Id*. at 795. This assertion was insufficient to establish probable cause to search the phone because it did not demonstrate the nexus between the phone and the alleged crime. *Id*. (warrant overbroad where the "application lacked any nexus between cell phones and marijuana possession").

In *Commonwealth v. Broom*, 52 N.3d 81, 89 (Mass. 2016), the court held that a warrant that police had executed to search a defendant's cell phone as part of a murder investigation was overbroad. The court observed that "[t]he properties of [a cell phone] render it 'distinct from the closed containers regularly seen in the physical world, [and] a search of its many files must be done with special care and satisfy a narrower and more demanding standard' than exists for establishing probable cause to search physical containers." *Id.* at 89–90. The court concluded that the affidavit law enforcement had submitted did not satisfy probable cause to search the phone because its statement that "there [was] probable cause to believe that the [defendant's] cell phone and its associated accounts . . . will likely contain information pertinent to this investigation" was "general" and "conclusory." *Id.* at 89.

State courts examining "training and experience" warrants to seize phones and computers are concluding similarly.[19] For example, in *Commonwealth v. White*, 59 N.E.3d 369 (Mass.

Cir. 2019) (cell phones are well-recognized tools of the trade for drug traffickers); *State v. Mansor*, 421 P.3d 323, 326, 344 (Or. 2018) (similar, under state constitutional law); Brief for ACLU of Mass. & Electronic Frontier Foundation as Amici Curiae Supporting Def., *Commonwealth v. Snow*, 160 N.E.3d 277 (Mass 2020) (SJC-12938) [brief attached at Appendix 528]; *United States v. Garay*, 938 F.3d 1108, 1113 (9th Cir. 2019) (Probable cause found in vehicular homicide case based on high-speed chase, driver's attempt to flee, discovery of drugs and cash on his person, discovery of loaded guns, ammunition, and cell phones inside car and affidavit stating that in officers' experience people who possess firearms "like to take pictures of [those items]" with their cell phones, and "will also communicate via text" regarding criminal activity.)

[19] *State v. Henderson*, 289 Neb. 271, 854 N.W.2d 616 (2014) (cellular telephone); *State v. Castagnola*, 145 Ohio St.3d at 18–24, 46 N.E.3d at 657–61 (computer); *Wheeler v. State*, 135 A.3d 282 (Del. 2016) (computer); *State v. Keodara*, 364 P.3d 777, 783 (Wash. App.

2016), the Massachusetts Supreme Judicial Court addressed a warrant where the defendant's cellular telephone was seized on the basis that (1) the officers had reason to believe that the defendant participated with others in committing a crime and (2) their training and experience in cases involving multiple defendants suggested that such defendants usually used their devices to communicate. The court explained that upholding the warrant would essentially allow police to obtain a warrant in every criminal case by simply stating that, in their experience, individuals use phones to conduct criminal activity. "If this were sufficient . . . it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search. *Id.* at 591–92 (citing *Riley*, 573 U.S. at 399 (only "inexperienced or unimaginative law enforcement officer ... could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone"); *see People v. Hughes*, 958 N.W.2d 98, 110 n.6 (Mich. 2020) [Appendix 49] ("[D]efendant thus raises a not-unreasonable concern as to the issuance of a warrant to search and seize cell-phone data based solely on the nature of the crime alleged.").

It's a slippery slope when courts automatically find probable cause to search electronic devices. In *United States v. Griffith*, 867 F.3d 1265, 1275 (D.C. Cir. 2017), police sought authorization to search a home because the cell phone was probably inside. The D.C. Circuit held that the government may not search a home for cell phones even though the officer suspects that the phone may contain evidence of a crime. The court characterized the government's argument as follows: because nearly everyone now carries a cell phone, and because a phone frequently contains all sorts of information about the owner's daily activities, if a person is suspected of a crime, that suspicion ordinarily justifies searching her home for any cell phones, regardless of whether there is any indication that she in fact owns one or has used it in an offense. This reasoning "would verge on authorizing a search of a person's home almost anytime there is probable cause to suspect her of a crime." *Id*.

In short, a factual nexus is constitutionally required and, as a growing number of cases recognize, it must be based on more than the fact that computers and phones are part of everyday life.

3. When Issuing Warrants Authorizing the Seizure of Electronic Data Stored Online, Courts Must Limit the Seizure by Category of Data, Date Range, and Other Filters.[20]

Courts may not issue warrants purporting to authorize seizure of all data from an electronic account (all-data or all-content warrants).[21]

2015), *review denied*, 377 P.3d 718 (Wash. 2016) (phone); *State v. Mansor*, 381 P.3d 930 (Or. 2016) (computers).

[20] The Fourth Amendment requires similar targeting in conducting the search.

[21] *See United States v. Blake*, 868 F.3d 960, 966–67 (11th Cir. 2017) (probable cause to search the Facebook account but the search warrants required the social media company to turn over virtually every type of data that could be located in a Facebook account without time limitation); *State v. Hamilton*, No. 6:18-CR-57-REW-10, 2019 WL 4455997 (E.D. Ky. August 30, 2019) (probable cause showed that suspects communicated over Facebook

While warrants must particularly describe the place to be searched and the thing to be seized, in the context of digital data, it is not always clear how to adhere to this constitutional safeguard. Electronic storage tends to intermingle evidence of a crime with non-responsive and innocent information. For information stored on hard drives or mobile phones, courts have generally been convinced that overseizure of the data is necessary to conduct a proper forensic search because investigators cannot meaningfully segregate responsive from non-responsive data on site. Thus, courts have permitted law enforcement to "seize first, search second"—authorizing broad seizures of stored data for logistical reasons, justified by constraints at the search stage.

Some courts have suggested that Federal Rule of Criminal Procedure 41 categorically permits police to overseize the full contents of social media and other cloud-storage accounts. *See, e.g.*, *In Matter of Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 11 (D.D.C. 2013). That view is not correct. The rule allows judges to authorize the overseizure of electronic storage media first, and contemplates later review of that data consistent with the warrant. But any overseizure must still be "reasonable" within the meaning of the Fourth Amendment. The rule does not (and constitutionally could not) authorize seizures of data that are unnecessary or unreasonable in the context of a particular investigation.

Because there is an administrative need for data overseizures in so many cases, the government regularly has "access to a larger pool of data that it has no probable cause to collect." *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (citing *Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (hereafter "*CDT*") (9th Cir. 2010) (en banc) (per curiam)). Where this is necessary, it is even more important that the search be constrained to limit exposure of this information to the government.

Whatever the merits of a *seize first, search second* approach in the context of computer hard drives, *see supra* Section III.A., the same considerations do not justify seizures of data in an email or social media account.[22] Obtaining every bit of information in an online

---

Messenger about drug deals, so information from Facebook Marketplace, "gifts," "pokes," all Facebook searches performed, groups, rejected "friend" requests, "friends" list user identification numbers, and his "check ins," were overbroad).

[22] Some courts have, however, resisted this approach. *In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. July 18, 2014) ("We perceive no constitutionally significant difference between the searches of hard drives … and searches of email accounts."). They have permitted boilerplate warrant language that seeks all-content, or an exhaustive list of categories of materials that comprise essentially everything ever amassed in an individual's digital life. *See, e.g.*, Snow, 160 N.E.3d at 286–87, 289 (search warrant allowed officers to search virtually every area on the cell phone, court held that suppression may be required because search warrant did not specify date parameters); *Search Warrant to Sony Interactive at 6–8, In the Matter of the Search of Information Associated with the Electronic Account for PlayStation User "Speedola20"*, No. 4:19-SW-00364-JTM (W.D. Mo. Oct. 22, 2019)

account will usually be unnecessary. The provider preserves account data after the receipt of a warrant, so time is no longer of the essence in the same way that it is when officers must seize a device from the suspect's possession. In addition to being able to preserve data, the service provider has the capability of filtering out irrelevant data. Investigators can work with providers to sort account data and ultimately hand over only responsive information. Providers are able to effectively distinguish images from text, find material by date, and filter conversations by participant or even keyword.

Notably, the means of hiding evidence on a hard drive are not currently possible in the context of a Facebook or other social media account. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017), *cert. denied sub nom*. *Blake v. United States*, 138 S. Ct. 753. Information associated with the account is categorized and sorted by the company—not by the user. Even sophisticated criminals cannot effectively hide evidence behind misleading file names or types online. "[T]here is no possibility that a user could have filed an incriminating photo as a 'poke,' and there is no chance that an incriminating message will be stored as a third-party password or a rejected friend request." *Shipp*, 392 F. Supp. 3d at 309. The platform organizes the information in such a way that even a technologically sophisticated criminal cannot effectively conceal information in a different category of information.

Seizing the entirety of online account data raises cybersecurity and oversight concerns as well as privacy considerations. Many of the information demands that officials list as part of common boilerplate should almost never be permitted, such as obtaining passwords and PIN codes. This information can be used to prospectively spy on account holders, a technique that likely requires a Title III wiretap warrant, not a Rule 41 warrant (or its state-law equivalent).[23] It risks abuse by enabling officers to repeatedly access accounts without judicial oversight. Passwords can also be misused to send fake messages, impersonate the account holder, or even create false evidence.

Nevertheless, for email or social media account data, investigators routinely obtain warrants for seizure of "all data," "all content," or an extensive boilerplate list of every and

---

(seeking the contents of all communications, drafts, passwords, security question answers, account records, purchase and payment information, likes, and more), available at https://www.documentcloud.org/documents/6565970-PlayStation-Seach-Warrant-Application.html.

[23] Fourth Amendment requires safeguards beyond traditional search warrants where surveillance consists of "a series [of intrusions] or a continuous surveillance" and not "one limited intrusion." *Berger v. State of New York*, 388 U.S. 41, 57 (1967); *See also* Orin Kerr, *A User's Guide to the Stored Communication's Act—And a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1232 (2004) (it is the functional equivalent of a wiretap if an agent installs software that copies incoming messages a few milliseconds after they arrive.)

any type of data that might exist for the particular provider. The data categories seek to capture everything—not just evidence of the crime under investigation.[24]

In one example, Los Angeles county investigators obtained a warrant for the entirety of a juvenile justice advocate's Google account on a speculative claim of obstruction of justice. *In re Search Warrant to Google for all Records Associated with Google Account scottarcla@gmail.com*, Case No. BH012910 (Cal. Super. Ct. Aug. 31, 2020) (hereafter "*Budnick* Opinion") [attached at Appendix 302–16]. The warrant sought all account data, phone information, passwords, PIN codes, credit card/payment data, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, financial records, photos, Play Store purchases, search history, and more.[25] The juvenile justice advocate, Scott Budnick, challenged the seizure, in part on overbreadth grounds. The court agreed that the warrant authorized the seizure of too much information—the warrant "made no attempt to limit the amount of information to be searched." *Budnick* Opinion at 10 [Appendix 311].[26] The ruling was specifically based on the particularity and notice requirements California's electronic privacy statute (CalECPA), but the traditional Fourth Amendment limitations would require the same result. *See* Brief of American Civil Liberties Union et al. as Amicus Curiae, *Budnick*, Case No. BH012910 (Cal. Super. Ct. Aug. 31, 2020) [brief attached at Appendix 272–301].

Thus, to the extent possible, warrants must contain limits on what data police can seize, especially from online providers where compliance with those limits is possible and will not unduly interfere with a legitimate investigation.

*4. Warrants Must Limit the **Categories** of Data to Be Seized from Social Media or Cloud-Storage Accounts to Those Responsive to Probable Cause.*

With respect to data in online accounts, a provider may be capable of initially sorting at least some non-responsive information out of the trove provided to law enforcement. For these reasons, a warrant authorization to seize social media data must be limited, where

---

[24] *In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted]*, 20 F. Supp. 3d 67, 724 (D.D.C. 2013) ("Generic and inaccurate boilerplate language will only cause this Court to reject future § 2703(d) applications.").

[25] See Cory Doctorow, *Search-Warrant Demands that Google Turn Over Account Info, Android Info, All Accounts and Passwords, Calendar, Contacts, Cloud docs, Financial Data, Photos, Location History, Search History, Call Records, etc*, BoingBoing.net (Dec. 17, 2019), https://boingboing.net/2019/12/17/organize-the-worlds-informatio-2.html; *see also In the Matter of the Search of Information Associated with Evernote Account Associated with Stephan4096@gmail.com*, No. 18-NJ-7130 (C.D. Ill. July 17, 2018), available at https://www.documentcloud.org/documents/6567399-Evernote-Executed-Search-Warrant.html.

[26] The *Budnick* court also held that there was no probable cause for that data seizure. *See* Appendix 261.

possible, to categories of information that are connected to probable cause in the specific case. In *United States v. Shipp*, 392 F. Supp. 3d 300, for example, a search warrant to Facebook demanded all of the suspect's personal information, activity logs, photos and videos, as well as materials posted by others that tagged the suspect, all postings, private messages, and chats, all friend requests, groups and applications activity, all private messages and video call history, check-ins, IP logs, "likes," searches, use of Facebook Marketplace, payment information, privacy settings, blocked users, and tech support requests. *Id.* at 303–06. This list was not limited to the types of information likely to provide evidence of the specific crime under investigation. The district court expressed "serious concerns regarding the breadth of [the] Facebook warrants." *Id*. at 307. Warrant-issuing courts "can and should take particular care to ensure that the scope of searches involving Facebook are 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" *Id.* (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)). If, for example, a case involves a conspiracy to sell drugs, the police do not need passwords, tagged posts, or "likes." In *Shipp*, the "all-content" warrant went far beyond those limits in purporting to authorize seizure of all this information.

To limit up front the information that the government gets access to, courts should reject "all-data," "all-content," or boilerplate warrants containing comprehensive lists of types of data in favor of a defined list of relevant categories of data tailored to the investigation at hand. For example, if the allegations are that a suspect sent photos of guns to prospective buyers over WhatsApp, the warrant can authorize a search of WhatsApp chats and associated photos sent through the application.

5. *Warrants Should Require Service Providers to* ***Filter Within Categories****, Including Use of Date Limitations, to Further Narrow the Amount of Non-Responsive Data Law Enforcement Officers Seize.*

Warrants to search cloud-stored electronic data should direct online service providers to reduce the amount of non-responsive data turned over to law enforcement to the extent possible.

First among these filters are date limitations. Email and social media accounts usually go back years and contain thousands or tens of thousands of messages with people uninvolved in any wrongdoing. In most cases, the vast majority of those messages will not be relevant to probable cause. If an offense allegedly took place in 2019, police may not need to obtain email from any other year, never mind from the inception of the account. For seizures of data from online service providers, it will almost always be possible to request materials from a limited data range. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad).

Narrow warrants can protect against searches for evidence of past crimes as well as against broad searches justified by probable cause for minor crimes. *Riley*, 573 U.S. at 399 (warrant necessary for this purpose). Depending on the service provider's functionality, police may not need to seize all messages in an email account. For example, in *In re Search of Info. Associated With Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 844 (D. Or. 2018), the warrant sought all emails associated with the suspect's account. The court held that the warrant was overbroad because Google is able to date-restrict the email content it discloses to the government, hewing more closely to probable cause. In *State v. Mansor*, 421 P.3d 313 (Or. 2018), the Oregon Supreme Court held that the warrant to search the defendant's computer should have been limited to search history on the day of a child's injury and death, not the weeks and months before the death, as the government requested. *Id.* at 343–44 (interpreting Article I, section 9 of the Oregon Constitution). Similarly, in *Commonwealth v. Snow*, 160 N.E.3d 277 (Mass. 2021), the Massachusetts Supreme Judicial Court found that a warrant to search the cell phone of a defendant accused of murder was insufficiently particular because it authorized a search without a temporal limit, even though the government argued "it was unknown 'when the weapon used was acquired and when any related conspiracy may have been formed.'" *Id.* at 282; *see also People v. Thompson*, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019) (warrant to search defendant's phones without a time limitation did not satisfy the Fourth Amendment's particularity requirement).

For the warrant to be particular, the proper date range should be set forth in the warrant, and not left to the officer's discretion. "A warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular." *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 459 (citation, quotation marks, and alterations omitted) (finding that the absence of a temporal limit on items to be searched "reinforces the Court's conclusion that the [ ] warrant functioned as a general warrant").

Thus, under the Fourth Amendment's particularity requirement, law enforcement may need to use date-range restrictions, or other limitations, to prevent the potential for "general rummaging" when searching electronically stored information such as email accounts. *See, e.g.*, *In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.*, 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016)*; In re [REDACTED]@gmail.com*, 62 F. Supp. 3d at 1104 (denying a search warrant for a particular email account because "there is no date restriction of any kind").

Other filtering can work too, and should be employed. Warrants authorizing account data seizures should not by default include data about third parties communicating with the account. The case *Facebook Opinion*, 21 F. Supp. 3d 1 (D.D.C 2013), contains several examples of investigator attempts to obtain information about people who were in contact with the defendant, without limitation. There, the government sought a warrant for "records relating to who . . . communicated with the user ID, including records about their identities and whereabouts." *Id.* at 4. It also sought "records, information, and items related to any organization, entity, or individual in any way affiliated with [the target]." *Id.* These requests would reveal names and locations of people as well as group membership lists. Without specific probable cause to obtain this information, the warrant would not only authorize raking through the target's personal relationships, but also reveal sensitive personal and

political information about third parties unsuspected of criminal behavior. As the court there said, "[d]epending on what the government found after a search of [the target] account, probable cause could exist to learn more information about another individual or a group. But no such probable cause existed for the initial foray into [the] Facebook profile, and it was therefore premature for the government to seek so much information about third parties." *Id.* at 7.

Keyword searches may be an option to further limit the data that a service provider discloses to law enforcement. The government must be required to narrow the data it seizes from online service providers by asking the provider to limit disclosures based on keywords, such as the name of a co-conspirator, a bank account number used for illegal proceeds, or reference to the address where a burglary took place.

For example, officers could easily limit the warrant to demand only messages between co-conspirators. If Bob and Alice are collaborating, Google may be able to parse just messages between those two, just as account holders can do when they search their inboxes. The government should also limit its acquisition to mail sent by the suspect, or exclude emails between suspects and their employers, identified attorneys, clergy, or spouses, or notifications from social media entities like Facebook or Twitter. *In the Matter of the Search of premises known as: Three Hotmail Email accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *7, *14 (D. Kan. March 28, 2016).[27] *See also In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145, 2014 WL 1377793 (D.D.C. April 7, 2014); *In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, Nos. 13–MJ–8163–JPO, 13–MJ–8164–DJW, 13–MJ–8165–DJW, 13–MJ–8166–JPO, 13–MJ–8167–DJW, 2013 WL 4647554 (D .Kan. Aug. 27, 2013).

Images may be another area where providers' built-in search capabilities enable more tailored data seizures. Google Photos is designed to do image searches. *About Google Photos*, Google, https://www.google.com/photos/about/ (explaining that photos saved to Google photos "are organized and searchable by the places and things in them—no tagging required"). Investigators might seek from Google only those photos that were taken at a particular location or that contain the image of a particular person of interest.

The main objection to having online service providers search for and disclose only a portion of online account data is that providers are poorly positioned to conduct investigations for law enforcement. Providers do not know the facts of the investigation and are not trained law enforcement actors. However, specifications such as data category limitations, time frames, email to/from limits, and photo searches need not require the provider to understand the investigation or exercise any discretion. The search terms could be clear, set by the investigators, and overseen by the issuing magistrate. Often, these advanced searches are well within the capability of the provider and require no

---

[27] The magistrate was overturned by the District Court, which ruled that the "seize first, search second" process did not require these limitations. *In the Matter of the Search of Information Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation*, 212 F. Supp. 3d 1023, 1037 (D. Kan. September 28, 2016).

investigatory expertise to perform. Investigators can then follow up on any leads by obtaining a second warrant.

The first step in protecting electronic privacy is to limit the amount of data available to government to that for which there is probable cause to search. Complexities include the ability to copy data without depriving the owner of it, absence of familiar real-world barriers to hiding incriminating evidence, and concerns about preservation. None of these complexities justify wholesale seizure of data in every case, especially not in the context of online accounts.

B. DATA SEARCHES

1. General Principles

Fourth Amendment protections are especially important at the search stage. Because warrants for digital information often allow investigators to seize a vast trove of data, the government is capable of examining far more information than is relevant to probable cause. This practice intrudes into intimate, constitutionally protected, private matters. Courts must ensure that, even when logistical necessities may justify the government's overbroad data seizures of digital devices in certain circumstances, the subsequent search is sufficiently narrow.

The Ninth Circuit has issued the most in-depth judicial discussion so far on the problem of restraining searches of intermingled evidence. In *Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, law enforcement officers obtained a warrant to search the electronically stored drug-testing records of ten Major League Baseball players. *Id.* at 1176. In executing the warrant, officials seized and examined the drug-testing records of hundreds of other players, who were not subject to the warrant, but whose records were intermingled with those of the ten players named in the warrant. Chief Judge Kozinski, joined by four other judges, recognized many of the Fourth Amendment problems with electronic searches, and *recommended* additional limitations that may be constitutionally necessary to render digital searches reasonable.[28] The Ninth Circuit did not *impose* these limitations on future searches, however.

The *CDT* analysis remains important and influential, but its suggested remedies are problematic.[29] Are they recommendations, or safeguards required by the Fourth

---

[28] First, magistrate judges should insist that the government forswear reliance on the plain view doctrine. Second, they should require the government to forswear reliance on any similar doctrine that would allow use or retention of data obtained only because the government was required to segregate seizable from non-seizable data. Third, the government should fairly disclose the actual degree of risk of concealment or destruction of evidence in the case at hand. Fourth, the judicial officer should insert a protocol to prevent agents from examining or retaining any data other than that for which probable cause is shown. Fifth, the court might require an independent search team, especially in cases where the party subject to the warrant is not suspected of any crime. Sixth, the government must destroy or return non-responsive data. 621 F.3d at 1180.

[29] Its factual assumptions are also inaccurate. *CDT* states that investigators will routinely need to seize all data because they are unable to reliably segregate responsive from non-

Amendment? Do judges have the authority to impose these restrictions? *See* discussion *supra* note 2. Do people retain an expectation of privacy in seized data? Is search, retention, use, or disclosure of that data a Fourth Amendment search or seizure subject to the constitutional requirement of reasonableness and a warrant? What happens when a search turns up evidence of a new offense?

There is case law responsive to some of these questions. For others, advocates and scholars have presented legal arguments, but courts have yet to consider or adopt those arguments. This section sets forth (1) evolving Fourth Amendment doctrine; (2) tools that magistrates should consider using to ensure that warrants they issue are properly executed; and (3) novel but persuasive legal arguments for more powerful warrants and judicial oversight. *United States v. Najar*, 451 F.3d 710, 714 (10th Cir.2006) (purpose of warrant requirement is to "buffer [ ] investigatory zeal with judicial oversight").

This section makes the following claims:

- Searches must be authorized and executed only to identify and disclose evidence of the crime for which there is probable cause;
- Courts must oversee data searches, which will require query logs, pre-search protocols, or similar transparency measures to ensure judicial control;
- Courts should impose restrictions on how officials may use non-responsive data seized during the execution of computer warrants, including by banning use of that data as evidence in court;
- Police may not search seized data for evidence of a new or different crime, especially not in the absence of a new warrant, or after a long period of data retention;
- When the case is over, non-contraband data must be returned and all data expunged.

2. *Courts Must Affirm That People Retain an Expectation of Privacy in Seized Data.*

Prosecutors have developed novel arguments to justify searches that exceed the limitations imposed by a properly issued warrant and probable cause, which some courts have adopted. The core of these arguments is that, once data is seized, the individual loses an expectation of privacy in it, including in the non-responsive data.[30]

---

responsive materials. As discussed above, that assumption is not always, and perhaps increasingly less, true. *See supra* Section III.A.

[30] *See, e.g.*, *Hughes*, No. 338030, 2018 WL 4603864, at *3 (Mich. App. Sept. 25, 2018) ("[B]ecause defendant's reasonable expectation of privacy had been extinguished through the issuance of a valid search warrant, he was not entitled to demand that any subsequent use of the same evidence be supported by a second search warrant."); *People v. McCavitt*, Supreme Court of Illinois No. 125550, Petition for Leave to Appeal p. 2 (questioning "whether the Fourth Amendment's warrant requirement even applies to police searches of

The consequences of adopting the view that one loses all expectation of privacy in seized data, even though the warrant limits the search of that data to evidence of a particular crime, are revolutionary. If true, law enforcement would search data outside of the strictures of the warrant, for evidence of any crime, because this examination is not a Fourth Amendment search. Since police routinely overseize data, a warrant to search for one crime would in effect be a warrant to conduct a general search of all the data for evidence of any crime, or merely for prurient interest. Warrants would mean nothing.[31]

By way of analogy, the mere fact that police executed a valid search of a house for evidence of one kind on one day does not permit them to return to search for evidence of other crimes thereafter on the theory that the original search eliminated the person's expectation of privacy. Searches of personal devices and data are no different in this fundamental respect.[32] Warrants permit officers to invade a legitimate expectation of privacy for a particular purpose—to execute a specific search—consistent with the restrictions on police power set forth in the Fourth Amendment. Those restrictions ensure that any invasion of privacy is reasonable, no more invasive than necessary, and justified under the circumstances. Consequently, a warrant does not extinguish a person's expectation of privacy wholesale, forever, and for all purposes. It permits a carefully limited intrusion. Ongoing retention of that data is a seizure subject to Fourth Amendment limitations. Searches for evidence of crimes not described in the warrant are unconstitutional because they are, in effect, warrantless searches—and warrantless searches are by definition unreasonable, subject to only a few narrow exceptions. *See Katz*, 389 U.S. at 357.

---

digital property when police are searching a digital copy."). *See also* Certification by Wisconsin Court of Appeals at 16, 23, *State v. Burch*, 961 N.W.2d 314 (Wis. 2021) (No. 2019AP1404-CR) ("the State contends that [police] examination of the download did not constitute a "search" under the Fourth Amendment because Burch gave up his expectation of privacy in the phone's contents when he consented to the … extraction [of data].")

[31] The amicus briefs attached in the appendix delve into the various iterations of this core idea. They include ACLU filings in the following cases: *Ganias II*, 824 F.3d 199 (2d Cir. 2016) (en banc) (years later investigators obtained warrant to search of seized documents for evidence against new suspect) [brief attached at Appendix 396]; *Hughes*, 958 N.W.2d at 105 (cell phone seized in drug trafficking investigation searched for evidence of armed robbery) [brief attached at Appendix 1]; *Illinois v. McCavitt*, No. 125550, 2021 WL 4898748 (Ill. Oct. 21, 2021) (post-acquittal, seized cell phone data searched for evidence of crimes against new victims) [brief attached at Appendix 81]; *Burch*, 961 N.W.2d at 316 (cell phone data seized pursuant to consent in hit-and-run investigation warrantlessly searched for evidence of murder) [brief attached at Appendix 199]; *see also* BIDMAS Letter (confirming that FBI uploads raw search warrant return data into centralized database for subsequent querying).

[32] While entering a home deprives the user of exclusive use of it for some period of time, which is not true of digital information, which can be freely used without dispossessing another. While this theory may be relevant to whether a second search of data is a *seizure* depriving the owner of the possessory interest in data, it is irrelevant to an assessment of the ongoing expectation of privacy.

3. *Warrants May Not Authorize Searches of Any or Every File, Especially as Forensic Tools Can Facilitate Narrow Searches Cabined to Probable Cause.*

Some courts have held that once there is probable cause to search an electronic device, the investigator may search every file on the device. For example, the Fourth Circuit has held that, "[w]hen a search requires review of a large collection of items, such as papers, 'it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" *United States v. Williams*, 592 F.3d 511, 519-20 (4th Cir. 2010) (so long as the Fourth Amendment's basic requirements of probable cause and particularity are met, the executing officers are "impliedly authorized . . . to open each file on the computer and view its contents, at least cursorily, to determine whether the file [falls] within the scope of the warrant's authorization), *affirmed by Cobb*, 970 F.3d at 329. This view has it backwards. The vast amount of stored personal data requires special judicial oversight and investigator restraint, not unlimited searching.

Increasingly, courts have followed *Riley* to hold that looking in the right place, not *every* place, is the only plan that makes sense and complies with the Constitution. *See, e.g.*, *Burns v. United States*, 235 A.3d 758, 775 (D.C. 2020) (warrant authorizing search for categories of data for which there was no probable cause was "constitutionally intolerable"); *People v. Musha*, 131 N.Y.S.3d 514, 683 (N.Y. Sup. Ct. 2020) (in a child abuse case, there was probable cause to search the phone's photographs, but not to examine web search history); *State v. McLawhorn*, 2020 WL 6142866, *24–*26 (Tenn. Crim. App. 2020) (cannot search entirety of phone to determine whether device has flashlight function); *State v. Bock*, 485 P.3d 931, 936 (Or. App. 2021) (warrant authorizing the search of a cell phone for circumstantial evidence about the owner and any evidence related to suspected criminal offenses, including unlawful firearm possession, was not sufficiently specific under state constitution's Fourth Amendment corollary); s*ee also In re United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1147–1151 (W.D. Wash. 2011) (application to search and seize "all electronically stored information . . . contained in any digital devices seized from [defendant's] residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods" was improper because it sought "the broadest warrant possible," and did not propose to use a search technique that foreclosed the plain view doctrine's application to digital materials).

The Fifth Circuit recently took *en banc* a case considering this question. In *United States v. Morton*, 984 F.3d 421 (5th Cir. 2021), *reh'g en banc granted*, 996 F.3d 754 (5th Cir. May 18, 2021), the Fifth Circuit panel held that the government properly obtained a warrant to search a cell phone for text messages, call logs, and contacts, but that the warrant did not establish probable cause to believe the evidence would be in the form of photographs. The photographs that the prosecution sought to enter into evidence were therefore suppressed, and the conviction was overturned. After *en banc* review was granted, we filed a brief arguing that (1) there was insufficient nexus between the crime under investigation and the cell phone to establish probable cause, *see infra* Section V.A.2, and (2) the FBI

should not have been able to search categories of data (photos) when there was no probable cause to believe that evidence of the crime would be contained in a photo.[33]

The Delaware Supreme Court has held that a warrant permitting search and seizure of "any/all data stored by whatever means" failed the Fourth Amendment and state Constitutions' particularity requirements. *Taylor v. State*, No. 91-2020, 2021 WL 4095672 (Del. Sept. 8, 2021). The court stated that it was "reluctant to make specific pronouncements about what is required in a search warrant for electronic devices for fear that [it] might tie the hands of investigators," but more specificity is required than simply identifying the smartphones to be searched and allowing all data "pertinent to the criminal investigation" to be searched. *Id*. at *9-10 "The free-ranging search for anything 'pertinent to the investigation' undermines the essential protections of the Fourth Amendment—that a neutral magistrate approve in advance, based on probable cause, the places to be searched and the parameters of the search." *Id*.

The counter-argument is that digital data for which there is probable cause to search may, to a human eye, look more or less the same as non-responsive off-limits information. For example, a word-processing document might contain text, images, or both—but a human observer may not readily anticipate which before opening the file. A suspect may obscure folders or misname files in order to hide them. Some courts have held that investigators therefore must be permitted to rifle through non-responsive intermingled information in order to find evidence. *United States v. Hill*, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (Kozinski, J.) ("There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."). A number of courts have held that such human review is reasonable, on the grounds that it is impossible to otherwise determine whether a file on its face may contain relevant evidence. *See id.*; *Williams*, 592 F.3d at 519–20; *Cobb*, 970 F.3d at 329.

Much mischief flows from this approach. Under this reasoning, a warrant authorizes police to examine, at least cursorily, every file on the computer. *Williams*, 592 F.3d at 521; *Cobb*, 970 F.3d at 326–29 (relying on *Williams* but noting that while the search was appropriate under the facts of the case, "the Fourth Amendment might require more specificity as to the place to be searched or the items to be seized in some computer searches . . . ."). In effect, this means that probable cause to search a computer for evidence of one crime necessarily gives officers permission to examine every file on the machine. Rather than proceeding cautiously because of the sensitivity and volume of information stored on a hard drive, this view throws caution away because of the intermingled nature of the data. Rather than imposing real-world-like considerations on the search – don't look in the medicine cabinet for a rifle – this digital exceptionalism amounts to a free-for-all.

Nor does this approach benefit investigators, who will inevitably be tasked with making sense of a flood of data, the vast majority of which has nothing to do with criminal activity. Of course, this is not how police actually conduct searches. Today, there are readily available forensic tools that do a better job than human review when (1) searching for information; (2) protecting non-responsive information from police; and (3) ensuring that

[33] Readers should be sure to check whether these pending cases have been decided before citing them.

evidence seized has not been tampered with or altered in the course of an investigation. Today's forensic software is capable of discerning between different types of files. Koepke, *supra* note 7; *In Matter of Search of Information Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.,* 21 F. Supp. 3d 1 ("[T]here has been a sea change in the manner in which computers, which now contain enormous amounts of data, are searched with technology assisted review replacing other forms of searching, including the once thought gold standard of file-by-file and document-by-document review."). So, the assumptions underlying the conclusion that probable cause to search a computer must mean permission to open every file have been undermined by subsequent technological and legal developments.

Forensic software offers law enforcement a tool for running particularized digital searches—that is, searches that are designed to reveal files and folders for which a warrant establishes probable cause. To be clear, forensic software examines every file as well as other data stored on a hard drive, and that examination is a Fourth Amendment search. But the search could be considered more *reasonable* because it becomes far less likely that non-responsive data will be exposed to investigators. Investigators should be obligated to use forensic software to conduct properly designed queries that limit the data investigators ultimately see.

Forensic tools also can empower judicial oversight and due process for criminal defendants. Magistrate judges overseeing the search can review logs of the queries to ensure that officer's searches were reasonably related to probable cause and not fishing expeditions or expressions of idle curiosity. Relatedly, the forensic software must be proven accurate, the defense team must have access to it, and must be able to replicate the searches to ensure that the evidence is not corrupted.

4. Whether Set Forth in the Warrant or Reviewed Post-Search, Courts Should Require Search Protocols and Query Logging to Ensure that Searches Adhere to Probable Cause and to Enable Judicial Oversight.

The Constitution requires some judicial oversight of government seizures and searches, but does not limit the specific means of conducting that oversight to the issuance and enforcement of constitutionally valid warrants. Magistrates have a number of tools at their disposal. For example, magistrates can impose search protocols, mandate query logging, use a "clean team" to segregate data, and/or require destruction of non-responsive information. The Fourth Amendment may not require use of these safeguards in all cases. But under the facts of any particular case, magistrates will have strong reasons to impose some of them, either to avoid an unconstitutional search under the facts of that case, or to enable and enhance judicial oversight. More, defendants can cite the availability of these additional oversight measures to argue that it was not necessary for the government to have conducted an overbroad search of their electronic information.

An important question is at what stage of judicial oversight courts should impose reasonable search limitations. Courts could consider imposing a search protocol upon issuance of the warrant. *See In the Matter of the Search of 3817 W. West End*, 321 F. Supp. 2d 953 (N.D. Ill. 2004) (warrant authorized seizure but forbade search without magistrate-approved search protocol). This is an approach Chief Judge Kozinski supported in his

concurrence to the en banc Ninth Circuit's per curiam ruling in *CDT*. The concurrence, joined by four other judges, advised that a "warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown." *CDT*, 621 F.3d at 1179 (Kozinski, C.J., concurring). All analysis of digital data requires investigators to make choices about what to review, since it is impossible to review everything. Search protocols can help ensure that these decisions are cabined to probable cause by including, for example, date limitations, appropriate keyword terms, or other relevant limitations. Including these protocols in the warrant itself cabins the officers' discretion, as warrants are supposed to do, and will go a long way towards protecting non-responsive data from exposure to police.

A recent district court case from Michigan helpfully illustrates how courts are now confronting these issues. In *United States v. Stetkiw*, No. 18-20579, 2019 WL 2866516 (E.D. Mich. July 3, 2019), the government insisted, and the court was concerned, that "individuals might hide information in a way that forces a protocol-bound investigator to overlook it," *id.* at *5. Nevertheless, the court found that "an *ex ante* 'minimization' requirement can address concerns about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of non-responsive [electronically stored information] encountered in a search." *Id.* (citing Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L.J. 49, 55 (2018)). The court concluded that *ex ante* procedures would have several advantages: they would minimize contentious *ex post* review in the suppression context; they would allow for case-by-case tailoring of warrants to uncover materials whose seizure is supported by probable cause; they would permit judicial conversation over appropriate limitations; and they would help prevent even inadvertent conversions of warrants into general warrants. *See id.* While the *Stetkiw* court did not maintain that *ex ante* protocols are required in every case, it did recommend that in order to avoid such protocols, the government "should demonstrate that the level of probable cause to search [electronically stored information] is high enough to justify a search without minimization." *Id.*

While some magistrates now will not issue a warrant without search protocols in place, federal circuit courts have so far rejected the view that search protocols are *required*. Orin Kerr, *Executing Warrants for Digital Evidence*, 48 Tex. Tech. L. Rev. 1, 8 (2015) (citing *Evers*, 669 F.3d at 653). The Ninth Circuit has expressed its *preference* for a search protocol and has emphasized that, even in the absence of an articulated protocol, "[t]he reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials *remains subject to judicial review*." *Hill*, 459 F.3d at 978 (emphasis added) (citation omitted).

Professor Orin Kerr offers a counter-view, arguing not only that imposition of a pre-search protocol exceeds magistrates' lawful power, but also that it is a bad idea. Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241 (2010).[34] Kerr

[34] Professor Paul Ohm wrote a response addressing Professor Kerr's argument. Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. in Brief 1 (2011).

argues that *ex ante* limits to ensure that digital search warrants do not become general warrants impose too heavy an administrative burden on magistrate judges. *See id.* at 1260–73. A magistrate judge has no way to know in advance what means of executing the warrant will end up being constitutionally unreasonable, given the unique facts of each specific investigation, the argument goes, and interfering with searches and seizures *ex ante* thus impedes the proper formation of other areas of Fourth Amendment doctrine through the appellate process. *See id.* at 1277–78. Kerr argues that limits are therefore better imposed by appellate courts after the search, as part of the Fourth Amendment reasonableness analysis and in light of the realities of a specific investigation. *Id.*

At least some of Professor Kerr's arguments do not hold up against modern forensic tools. Kerr asserts that warrants should not set forth only narrow categories/limits on documents to be searched for as part of the particularity requirement. The simplest limitation set forth above is a date range. Kerr says that searching for files only with a known date parameter *could* work, but agents will not be able to know with certainty that they have found all responsive files, since files' metadata can always be changed. As a result, a negative result for a particular query never offers *complete* assurance that the evidence isn't there. But as set forth above, forensic tools today are designed with these kinds of data obfuscation techniques in mind and effective masking will be difficult, if not impossible. *See* discussion *supra*, Section III.C.[35] Kerr's concern that search protocols make investigations too difficult for police is misplaced today.

Regardless of whether courts should impose search protocols *before* issuing warrants, magistrates ought to require that investigators keep query logs documenting their searches. These search logs should be returned as part of the warrant inventory. This would allow judges to review these logs when a search warrant is returned and provide the information to defendants who may seek to suppress evidence. Search queries put both court and counsel in a position to review the search after the fact to ensure that it was scoped to probable cause. *See, e.g.*, *In re Search Warrant*, 71 A.3d 1158, 1184 (Vt. 2012); *CDT*, 621 F.3d at 1178–79. They are an effective way for courts to exercise their obligation to ensure that searches and seizures are constitutional, with no significant counter-arguments.

5. A Court Could Require an Independent Review Team, "Clean Team," or Special Master to Review Seized Evidence.

A warrant-issuing court might require the use of independent review teams to "sort[], segregat[e], decod[e] and otherwise separat[e] seizable data (as defined by the warrant) from all other data," so as to shield investigators from exposure to information beyond the scope of the warrant. *CDT*, 621 F.3d at 1179 (Kozinski, C.J., concurring). This prescription should be considered by magistrates and may, in certain factual circumstances, be required for a search to be reasonable and thus lawful. Clean teams are relatively common when investigators search an attorney's office or some other stash of presumptively privileged documents. But magistrates also should consider use of a clean team when investigators seize a voluminous amount of private data some of the data is particularly sensitive; the data is likely to include information from or about people who are not suspects; the search covers a long time-period; there is a risk of hidden or concealed evidence that requires

[35] *See* Koepke, *supra* note 7.

more extensive human examination; or in other similar circumstances. As Judge Kozinski urged in his *CDT* concurrence:

> [T]he warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown. The procedure might involve . . . a requirement that the segregation be done by specially trained computer personnel who are not involved in the investigation. In that case, it should be made clear that *only* those personnel may examine and segregate the data. The government should also agree that such computer personnel will not communicate any information they learn during the segregation process absent further approval of the court.
>
> At the discretion of the issuing judicial officer, and depending on the nature and sensitivity of the privacy interests involved, the computer personnel in question may be government employees or independent third parties not affiliated with the government. . . . Once the data has been segregated (and, if necessary, redacted), the government agents involved in the investigation should be allowed to examine only the information covered by the terms of the warrant.

CDT, 621 F.3d at 1179.[36] Clean team review on its own does not fully protect the data owner's privacy in that there are still third parties—and likely, government agents—reviewing their sensitive information. However, it does help ensure that digital search warrants are not a bonanza for law enforcement. It also better aligns incentives for investigators with courts' interest in ensuring that searches are scoped to probable cause: if irrelevant information will not be shared with law enforcement, there is less reason for clean teams to search for and examine it in the first place.

Given that the number of electronic searches is likely to grow exponentially, as a policy matter it could be useful to more formally institutionalize judicial oversight and data segregation. With the evolution of novel and complex surveillance techniques such as geofencing, reverse keyword warrants, Stingray use, and encryption backdoors, a dedicated class of magistrates whose main job is to approve and oversee novel technological investigative techniques could be in order.

6. *Police May Search for Evidence Only of the Probable Cause Crime, and Additional Searches Require a Second Warrant, at the Very Least.*

Well-established in case law is that police may only search seized data for evidence of the crime for which they have probable cause and a warrant. Nevertheless, we have seen several recent cases in which the government raised a host of reasons why such searches would be permissible—from a lack of expectation of privacy, to application of a "second look" doctrine, to the classification of seized data as merely "police records." These efforts should always fail.

---

[36] The concurrence in *CDT* went on to recommend that, absent further judicial authorization, any remaining copies in the government's possession of seized data should be destroyed. *Id.*; *See also infra* Section V.B.9.

In *United States v Carey*, 172 F.3d 1268, 1270 (10th Cir. 1999), a police officer searched a laptop for evidence of drug distribution pursuant to a warrant. While searching the laptop, the officer stumbled upon child sexual abuse materials (CSAM). *Id.* at 1271. At this point, he began searching for and opening files he believed were likely to contain CSAM, instead of continuing to search only for evidence of drug distribution. *Id.* at 1273. The Tenth Circuit held that the officer's "unconstitutional general search" violated the suspect's expectation of privacy in data not described in the warrant, and suppressed the evidence. *Id*. at 1276.

In contrast, in *United States v Walser*, 275 F3d 981 (10th Cir. 2001), the facts were similar to *Carey*, but the investigator, upon unexpectedly finding child abuse images, "immediately ceased his search of the computer hard drive and . . . submit[ted] an affidavit for a new search warrant specifically authorizing a search for evidence of possession of child pornography," *id.* 984–85. Because the officer did not search for evidence of the new crime of possession of illicit images without authorization from the magistrate in the form of a warrant based on probable cause, the materials were properly admitted into evidence. *Id*. at 987; *cf. United States v. Schlingloff*, 901 F. Supp. 2d 1101 (C.D. Ill. 2012) (unconstitutional search when agent stumbled on suspected CSAM, briefly viewed two files to confirm they were videos of child pornography, and only then applied for a search warrant).

At the very least, *Carey* and *Walser* mean that before police may search electronic data for evidence of a crime not identified in the warrant, they must first obtain a new warrant. (Below is a discussion of whether and when a second warrant can constitutionally authorize a new search. *See* discussion *infra* Section V.C.3.)

For example, the Michigan Supreme Court held in *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020), that police were not permitted to search the suspect's digital data for evidence of a crime not identified in the warrant. Quoting *Riley*, the court rejected the state's extreme argument

> that it is always reasonable for an officer to review the entirety of the digital data seized pursuant to a warrant on the basis of the mere possibility that evidence may conceivably be found anywhere on the device or that evidence might be concealed, mislabeled, or manipulated. Such a *per se* rule would effectively nullify the particularity requirement of the Fourth Amendment in the context of cell-phone data and rehabilitate an impermissible general warrant that "would in effect give police officers unbridled discretion to rummage at will among a person's private effects."

Id. at 541–42 (quoting *Riley*, 573 U.S. at 399). A seizure deprives an individual of control over their property but does not reduce their reasonable expectation of privacy in the contents of the property. *See Horton*, 496 US at 133. That is why, "[e]ven when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package." *United States v Jacobsen*, 466 US 109, 114 (1984) (footnote omitted). Warrants require probable cause and particularity precisely *because* searching for evidence of an unrelated crime is not permitted, even when the object is lawfully seized. In *Hughes*, the Michigan Supreme Court advised that lower state courts will have to decide, under the totality of the circumstances, whether a police search of

digital data was reasonably directed toward finding evidence of the criminal activities alleged in the warrant in order to determine the admissibility of evidence of a different crime obtained without a second warrant. *Hughes*, 958 N.W.2d at 120–21.[37]

In *State v. Burch*, 961 N.W.2d 314 (Wisc. 2021) [Appendix 199], officers obtained cell phone data pursuant to consent in the context of a hit-and-run investigation. After the phone owner was cleared of the hit and run, he became a suspect in a murder. The law enforcement agency that initially seized the phone data retained a full forensic copy of the data, which it provided to a different law enforcement agency in connection with the murder investigation. The second agency then searched the phone data for evidence of the murder, finding location data that put the defendant in proximity to the victim at relevant points in time. Burch challenged the state appeals court's ruling that "the sharing of such information, without first obtaining a warrant, is a common and long-understood practice between related departments." *Id.* at 317–18 (citation omitted) [Appendix 206]. The Wisconsin Supreme Court resolved the case on good faith exception grounds rather than considering whether Burch lost his expectation of privacy in his cell phone data once it was seized.[38] *Id.* at 321–22 [Appendix 211–12].

In a similar case, *People v. McCavitt*, No. 125550, 2021 WL 4898748 (Ill. Oct. 21, 2021) [attached at Appendix 125], law enforcement obtained a search warrant to investigate a police officer for several crimes against a single victim. That investigation led to criminal charges, and eight months later, the government's case against the officer ended in a jury's acquittal. The day after the acquittal, the police—still in possession of the defendant's hard drive under the first warrant—conducted a new, unwarranted search of the hard drive data, this time looking for evidence of different crimes against additional victims. In the course of conducting that new search, an analyst viewed child pornography. After pausing the search, the police sought and obtained a new warrant to search for evidence of child pornography, and the state charged the defendant again, ultimately obtaining a conviction. The appellate court reversed, holding that the Fourth Amendment barred the state's warrantless post-acquittal search for new evidence. *See People v. McCavitt*, 145 N.E.3d 638 (Ill. App. 2019), *appeal granted*, 147 N.E.3d 692 (Ill. May 27, 2020). Now, the state

---

[37] The opinion is strong on the principle that searches must adhere to probable cause, but suggests that the Court would apply the plain view doctrine if the police *inadvertently* found additional evidence, and would permit at least some retention of the data such that it would remain available for a second search with a warrant. *Hughes*, 958 N.W.2d at 122 & n.25 [Appendix 71]. *But see CDT*, 621 F.3d at 1178 (Kozinski, C.J., concurring); *State v. Bock*, 483 P.3d 931 (Or. App. 2021) (holding plain view exception cannot be reconciled with the Oregon Constitution's Fourth Amendment analogue in the context of electronic searches); *infra* Section V.B.7.

[38] The case also involved the issue of whether the initial seizure of the cell phone information pursuant to consent was overbroad. The ACLU, the Electronic Frontier Foundation, and the Electronic Privacy Information Center argued in an amicus brief that a lay person's understanding of consent as applying to particular categories of information rather than the entirety of a phone's content should control. *See* Appendix 81–125.

supreme court is considering whether that second search was unconstitutional. *See* Appendix 81–124.

In each of these cases, investigators conducted an impermissible second warrantless search for evidence of a different crime. Such subsequent warrantless searches illustrate that the purpose of warrants—namely, limiting police searches in accordance with probable cause or consent—would be subverted if courts were to adopt the extraordinary argument that people entirely lose their expectation of privacy once data is seized.[39]

At least one court, now reversed, has held that even a second warrant may not be justification enough to search non-responsive information retained by the government. *See United States v. Ganias* (*Ganias I*), 755 F.3d 125 (2d Cir. 2014) [attached at Appendix 430], *rev'd en banc on other grounds by Ganias II*, 824 F.3d 199 (2d Cir. 2016) [attached at Appendix 467]. In *Ganias*, the FBI seized an accountant's digital files in connection with an investigation in which the accountant was not a suspect. The government did not delete or return information outside the scope of the warrant and, about two-and-a-half years later, obtained a separate warrant to investigate the accountant for tax improprieties. A Second Circuit panel held that the years-long delay in deleting non-responsive information violated the Fourth Amendment, and, since the government should not have had the information in the first place, the violation was not cured by officers' having obtained a second warrant to search Ganias's files in connection with the tax evasion case.

> If the 2003 warrant authorized the Government to retain all the data on Ganias's computers on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a general warrant. The Government's retention of copies of Ganias's personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time. This combination of circumstances enabled the Government to possess indefinitely personal records of Ganias that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files.

Ganias I, 755 F.3d at 137. The en banc Second Circuit reversed on the grounds that the search, even if illegal, was in good faith because it was performed pursuant to a warrant. *Ganias II*, 824 F.3d at 209. But the panel's reasoning remains persuasive. People have an ongoing Fourth Amendment right in how their data is used, analyzed, stored, shared, and ultimately deleted, including post-seizure.

---

[39] A related issue is whether people have an expectation of privacy in their online account data given that most service providers' terms of service reserve for the provider the right to scan and access user data that appears to constitute evidence of a criminal offense or violation of the providers' policies. The issue generally arises when law enforcement seizes account data and searches it without a warrant. The ACLU and partner organizations have filed multiple briefs arguing that terms of service permitting provider monitoring do not vitiate constitutional protection for that data. *See, e.g.*, *Wilson*, 13 F.4th 961 (9th Cir. 2021); *Wolfenbarger*, No. 5:16-CR-00519-LHK-1 (N.D. Cal. verdict rendered Aug. 8, 2021).

How then to reach the *Ganias I* result? An ongoing expectation of privacy in digital papers and effects means that the Fourth Amendment continues to regulate government handling of electronic information even after it is initially seized. This is important because, given how inexpensive digital storage is, the government can easily hold on to the digital data of people previously suspected of crimes, essentially creating permanent digital dossiers. Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002). Subsequent use of this stored data enables every computer warrant that is narrow in theory to become general in fact, in contravention of the longstanding principle of proportionality established in *Terry v. Ohio*, 392 U.S. 1, 20 (1968) (The question is not just "whether the officer's action was justified at its inception," but also "whether it was reasonably related in scope to the circumstances which justified the interference in the first place."). *See also Mansor*, 421 P.3d at 344.

While courts are increasingly accepting this conclusion, there are as yet no answers to a series of follow-on questions. For example, how long may police retain data? One view is that at a certain point—two-and-a-half years in *Ganias I*—the government's ongoing retention of data is no longer reasonable, and thus violates the Fourth Amendment. No second warrant can cure the problem of the overlong data retention, and without the data, the warrant would be pointless.

This is essentially the argument that the ACLU presented in *Hughes*, 958 N.W.2d 98 [brief attached at Appendix 1]; *Burch*, 961 N.W.2d 314 [brief attached at Appendix 1]; and *McCavitt*, 2021 WL 4898748 (Ill. Oct. 21, 2021) [brief attached at Appendix 81]. The argument is attractive because it is relatively straightforward, grounded in existing Fourth Amendment law, and does not require the creation of new, digital-specific doctrine. However, the argument leaves open the question of what constitutes the time-frame after which a secondary search of retained, non-responsive data is beyond saving. Scenarios like that in *McCavitt* are relatively straightforward: the government's right to retain data ceases at the point that a person is acquitted. It is less clear how long the government may retain non-responsive data after a *conviction*. After all, a defendant could appeal their conviction, in which case the data would potentially remain relevant as long as proceedings are ongoing. *See, e.g.*, *Hughes*, 958 N.W.2d 98 [Appendix 39–40].

Generally, courts need not depart from longstanding Fourth Amendment law to reach the right result. An additional class of arguments asserts that "digital is different," and so the Fourth Amendment demands use restrictions on seized electronic data that are distinct from the way the Constitution treats analog evidence. Pursuing this line of reasoning leads to arguments that Fourth Amendment law must diverge from tradition and impose restrictions on the ways that non-responsive data obtained in an electronic search and seizure may be used. The "digital is different" arguments enjoy strong support from recent Supreme Court precedent and should be raised in every case. The next sections of this paper address ways that searches and seizures should be restricted based on those arguments.

C. EXPLOITATION OF SEIZED NON-RESPONSIVE DATA

1. Courts Should Prohibit Use of Non-Responsive Data as Evidence of Other Offenses.

To this point, this memo argues that (1) searches must be only for evidence of the probable cause crime; (2) searches must be narrowly executed; (3) at the very least, another warrant is required to search seized data for a different crime; and (4) at some point the ongoing retention of data is unreasonable, the data must be deleted, and even a search pursuant to a second warrant is unconstitutional.

This argument has the merit of being soundly based in current Fourth Amendment jurisprudence. Of course, there are ongoing uncertainties that the law will need to address via ongoing litigation. For how long can police retain data? Under what conditions can law enforcement search the data? Does it need a new warrant? When can police share the data? Are there limits on how the data can be used? But these questions can be worked out in litigation, likely under the "reasonableness" test that is core to current Fourth Amendment jurisprudence.

What remains clear is that even if law enforcement obeys these strictures, there will often be a bonanza of digital information just by the very nature of electronic data storage. Even narrow searches may inevitably reveal personal and non-responsive information. This problem is exacerbated by the fact that in some number of investigations, law enforcement may need to conduct broad searches to ensure that it finds all evidence.

So how should courts ensure that electronic searches—which, again, always entail intermingled information, overseizure, and search complexities—do not become data windfalls for law enforcement? More specifically, how should Fourth Amendment doctrine apply to the non-responsive data investigators will inevitably encounter during the forensic process?

Professor Kerr has argued for strict restrictions on the use of seized data. Police, he argues, cannot be expected to search narrowly to find evidence of the crime under investigation. Evidence is everywhere, and hidden, and neither magistrates nor officers are in a good position ahead of time to detail how investigators will effectively find it. So, to address the privacy invasion that will stem from these searches, Kerr advocates for the imposition of *use restrictions* on seized data. His view is that "digital is different" and the Fourth Amendment must impose use restrictions on seized electronic data, in a way that is different from how analog evidence is treated. To ensure that broad digital searches adhere to Fourth Amendment principles, Kerr has argued that (1) courts should exclude evidence police stumble upon, even if it would otherwise be admissible under the plain view doctrine, and(2) that courts should impose a general use restriction on any non-responsive data obtained in an electronic search and seizure.

The doctrinal reasoning behind this view is that, although the seizure of non-responsive files is reasonable when needed to effectuate the search for responsive files, retention of the files is an "ongoing seizure." While initially justified, the subsequent use of seized non-responsive files transforms the nature of the seizure and renders it constitutionally unreasonable. Kerr, *Executing Warrants for Digital Evidence*, 48 Texas Tech. L. Rev. at 25–29.

This view requires courts to adopt a rule that does not currently exist in Fourth Amendment jurisprudence. It also leaves open some of the more difficult questions raised above, such as whether a use restriction only bars use of non-responsive data revealed in executing the warrant or whether it should also bar the execution of additional warrants based on independent probable cause, as in *Ganias*.

Ultimately, Kerr's argument might be stronger than the one we have previously presented in *Ganias*.[40] The government could never get a second warrant to review seized data, regardless of how little time has passed. While Kerr would allow use to address exigencies, he would not permit whatever data is found to form the basis of a new probable cause finding.

In other ways, Kerr's view is less protective. Of course, allowing a full search does not actually protect a person's privacy. Investigators will still learn intimate information about the individual's life. Limiting the use of that evidence is at best an incomplete remedy. If the person is not charged with a crime, use restrictions are irrelevant. If evidence is discovered, investigators will be incentivized to use "parallel construction," a shady technique where the government manufactures an alternative discovery route for evidence obtained through illegal means, or via techniques the government would rather not have publicly known or reviewed by a court. Jennifer Granick, American Spies 178, 224 (2017). Further, there is the danger that, with enough information, police could find something that would support their prosecution of the original crime. "If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him." Armand Jean du Plessis, Cardinal-Duc de Richelieu et de Fronsac as cited in Jehiel Keeler Hoyt, The Cyclopedia of Practical Quotations 763 (1896).

2. Courts Should Limit the Plain View Doctrine.

Another approach to limit exploitation of seized data is for courts to reject application of "plain view" exception to the Fourth Amendment's warrant requirement. *See* Orin Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 314–17 (2004); Orin Kerr, *Searches and Seizures in a Digital World*, 118 Harv. L. Rev. 531, 582–84 (2005); *but see* Kerr, *Executing Warrants*, 48 Tex. Tech. L. Rev. at 20.[41] The plain view exception allows government agents to seize evidence or contraband without a warrant when the agents have viewed it lawfully and its incriminating nature is immediately

---

[40] Advocates arguing for use restrictions should start by thoroughly reading Kerr's article.

[41] Kerr's position has evolved and, as of this writing, he has concluded that use restrictions—not eliminating the plain view exception for digital searches—are the most sensible way to ensure that electronic searches do not become the equivalent of general warrants. Kerr, *Executing Warrants*, 48 Tex. Tech. L. Rev. at 23–24 (questioning whether eliminating the plain view doctrine will accomplish the goal of restricting government access to non-responsive data as defendants may first have to prove that the use of any data observed outside the initial warrant constitutes an additional seizure of that data, and courts have not yet held that data is seized anew whenever it is used.) In his opinion, a better course is to impose use restrictions on seized data.

apparent. The plain-view doctrine developed in cases involving physical-world seizures, where evidence is tangible and discrete.

Searches of digital information are a poor fit for the plain-view exception, in part because the justifications underlying the exception largely do not apply in the digital context. First, officer safety is not implicated in a controlled environment like an off-site forensic laboratory. *See generally* David H. Angeli & Christina M. Schuck, *The Plain View Doctrine and Computer Searches: Balancing Law Enforcement's Investigatory Needs with Privacy Rights in the Digital Age*, 34 Champion 18, 23 (Aug. 2010). Unlike a physical object, such as a knife or gun, *see, e.g.*, *United States v. Bishop*, 338 F.3d 623, 628–29 (6th Cir. 2003), the digital data stored on a computer hard drive cannot physically endanger anyone, *see Riley*, 573 U.S. at 386–87. Second, evidence preservation is not at risk in a typical computer search, which normally begins with the creation of a "bitstream" copy of the target hard drive. Third, where the computer hard drive is preserved, the police have ample time to obtain additional warrants (say, for evidence of an unrelated crime) without risking evidence destruction. *See, e.g.*, Christina M. Schuck, *Note: A Search for the Caselaw to Support the Computer Search "Guidance" in* United States v. Comprehensive Drug Testing, 16 Lewis & Clark L. Rev. 741, 760–61 (2012).

In order to apply the plain view exception, first, law enforcement's observation of the plain-view evidence must have taken place after an initially lawful intrusion (based on, for example, an existing warrant or exigency). *See United States v. Sifuentes*, 504 F.2d 845, 848 (4th Cir. 1974) (citing *Coolidge*, 403 U.S. at 466). And the fact that a warrant exists to search for some material on a computer does not automatically entitle the government to review *all* of the material on that computer for the reasons set forth above. The search must at the very least be particularized and not overbroad in accordance with the foregoing principles.

Second, the evidence and its incriminating character must be "obvious to the senses"—that is, there for the seeing and out in the open, rather than obscured or hidden. *Id*. at 848. On manual review, the incriminating nature of digital evidence may not immediately be "obvious to the senses" because file types, names, and sizes do not necessarily reveal their contents. *Cf. United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085, 1146 (9th Cir. 2008) (Thomas, J., concurring in part and dissenting in part), *modified on reh'g en banc*, 579 F.3d 989 (9th Cir. 2009).

So far, no court has rejected application of the "plain view" exception to the Fourth Amendment's warrant requirement, though there are strong arguments for them to do so. *See, e.g.*, Brief for the ACLU, ACLU of W. Va. as Amici Curiae Supporting Appellant, *Cobb*, 970 F.3d 319 [attached at Appendix 317–354]; *see also* Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. at 576–77 ("The dynamics of computer searches upset the basic assumptions underlying the plain view doctrine. More and more evidence comes into plain view, and the particularity requirement no longer functions effectively as a check on dragnet searches. In this new environment, a tightening of the plain view doctrine may be necessary to ensure that computer warrants that are narrow in theory do not become broad in practice.").

3. *The Government Must Segregate and Destroy Non-Responsive Data.*

Regardless of whether use restrictions are generally imposed, at some point, a person's privacy and possessory interests in their data should dominate, and even a second warrant cannot justify a search of data that the government no longer has a lawful interest in retaining.

To effectuate the Fourth Amendment's guarantee against unreasonable seizures, courts should impose limits on how long the government may store data it lawfully obtains. In *Andresen v. Maryland*, 427 U.S. 463 (1976), the Supreme Court affirmed that with respect to papers that exceeded the scope authorized by the government's search warrant, "the State was correct in returning [some of] them voluntarily and the trial judge was correct in suppressing others," *id*. at 482 n.11.

In the Second Circuit's *Ganias* case, the panel held that "[t]he Government's retention of copies of Ganias's personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time." *Ganias I*, 755 F.3d at 137.

Conditions other than the passage of time should also trigger an obligation to destroy seized data. *Compare Ganias I*, 755 F.3d 125 to *Hughes*, 958 N.W.2d 98, *McCavitt*, No. 125550, 2021 WL 4898748 (Ill. Oct. 21, 2021), and *Burch*, 961 N.W.2d 314. In *Hughes*, the defendant had already pled guilty to the first crime; in *McCavitt*, the defendant was acquitted (though an internal affairs investigation was reinitiated at that point); in *Burch*, the defendant was no longer a suspect in the initial investigation by the time the second investigation began. Courts have not begun to consider the question of whether any of these events—conviction, acquittal, or the closure of an investigation—trigger an obligation to return or destroy data so that police agencies are not stockpiling private information. Clearly acquittal should terminate any government right to access information: The case is definitively over. And while it is sometimes difficult to identify the end of an investigation, the same principle holds true in that context. There may be some reason to keep information post-conviction—for example, where the information is relevant to an appeal. But the government should have to demonstrate its obligation to preserve digital information in order to avoid a deletion requirement.

This is not a radical point of view. Even the Department of Justice has conceded that the government has a duty to purge non-responsive files. *See Ganias II*, 824 F.3d at 238 (Chin, J., dissenting) (government agent acknowledged he should have returned or destroyed non-responsive items after a 'reasonable period' of off-site review). Lastly, several federal courts have denied warrant applications on the grounds that the government had inadequately addressed the Fourth Amendment's requirement that it purge non-responsive data. *See In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 80 (D.D.C. 2014); *In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1, 9 (D.D.C. 2013); *In re Nextel Cellular Tel.*, No. 14-MJ-8005-DJW, 2014 WL 2898262, at *10–*11 (D. Kan. June 26, 2014); *Matter of the Search of Apple iPhone*, IMEI 013888003738427, 31 F. Supp. 3d 159, 165–66 (D.D.C. 2014); *Matter of Search of ODYS LOOX Plus Tablet Serial No. 4707213703415*, 28 F. Supp. 3d 40, 45 (D.D.C. 2014).

And yet, it is not clear whether government agents are following these prescriptions.[42] Reliable information about how law enforcement handles stored data is scarce. Magistrates can help cure this problem by imposing data retention limits, but more transparency would be of great assistance.

VI. SUMMATION

Data seizures must be permitted only when there is a case-specific reason to believe that evidence of the crime under investigation exists among the data to be seized. Courts should require police to use available tools—for example, category, date, and keyword filters—to limit both data seizures and data searches. Proper use of forensic tools can further limit exposure of private information to police officers and also enable judicial oversight of searches. Data should be segregated and the non-responsive data should be sequestered and ultimately returned or deleted.

People retain an expectation of privacy in their digital data after it is seized, and searches must be regulated accordingly. The Fourth Amendment's particularity and overbreadth rules apply in the digital context to ensure that non-responsive data remains private to the extent possible. There should be no second searches, at least not without a second warrant. And in conducting searches, agents must act in a way that is calculated to get evidence of the probable cause crime and, to the fullest extent possible, nothing more. Rather than defer to agents' judgment, courts must use the tools at their disposal to ensure this outcome.

The legal arguments offered in this paper and in the amicus briefs attached as appendices are meant as a resource for lawyers and judges to adapt and use as courts consider the scope and extent of protection that the warrant requirement gives to digital data.

---

[42] *See, e.g.*, Section III.E *supra*; *see also* BIDMAS Letter.